

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-344444

(43)Date of publication of application : 29.11.2002

(51)Int.Cl.

H04L 9/32

G06F 12/14

G06F 15/00

G06F 17/60

(21)Application number : 2001-148576

(71)Applicant : SONY CORP

(22)Date of filing : 18.05.2001

(72)Inventor : FUKUDA JUNKO

IHARA KEIGO

SUEYOSHI TAKAHIKO

AYATSUKA YUJI

MATSUSHITA NOBUYUKI

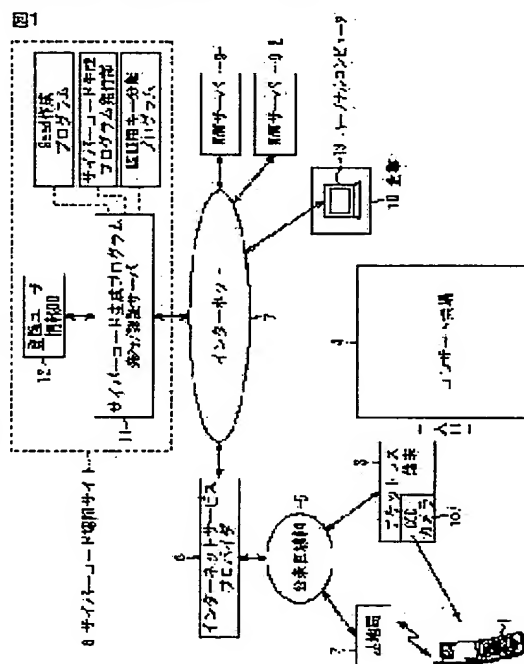
REKIMOTO JIYUNICHI

(54) INFORMATION PROVIDING DEVICE AND METHOD, INFORMATION PROCESSING DEVICE AND METHOD, INFORMATION AUTHENTICATING DEVICE AND METHOD, AUTHENTICATING SYSTEM, RECORDING MEDIUM AND PROGRAM OF THEM

(57)Abstract:

PROBLEM TO BE SOLVED: To make a program itself function as an authentication key.

SOLUTION: A cyber-code authenticating site 8 prepares a cyber-code generation program based on a user ID, a random number, and the present time, and transmits it to a portable telephone set 1. The portable telephone set 1 executes the received cyber code generation program, and generates and displays a cyber code. A ticketless terminal 3 images the cyber-code displayed at the portable telephone set 1 by a CCD camera 107, and transmits the recognized code number to a cyber-code authentication site 8. The code-code authentication site 8 retrieves the random number and the time information from a registered user information DB 12, based on the user ID included in the code number, and prepares the cyber-code generation program gain. Then, the user is authenticated from the code number of the cyber-code obtained by executing the prepared program.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

THIS PAGE LEFT BLANK

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

特許庁 登録部 第1部

THIS PAGE LEFT BLANK

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2002-34444

(P 2002-34444 A)

(43) 公開日 平成14年11月29日 (2002. 11. 29)

(51) Int. Cl.	識別記号	F I	テーマコード (参考)
H 0 4 L	9/32	G 0 6 F	12/14 3 2 0 F 5B017
G 0 6 F	12/14 3 2 0		15/00 3 3 0 A 5B085
	15/00 3 3 0		17/60 1 4 0 5J104
	17/60 1 4 0		1 4 6 A
	1 4 6		5 0 6
審査請求	未請求	請求項の数 2 4	O L (全 2 9 頁) 最終頁に続く

(21) 出願番号 特願2001-148576 (P2001-148576)

(22) 出願日 平成13年5月18日 (2001. 5. 18)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 福田 純子

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 井原 圭吾

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

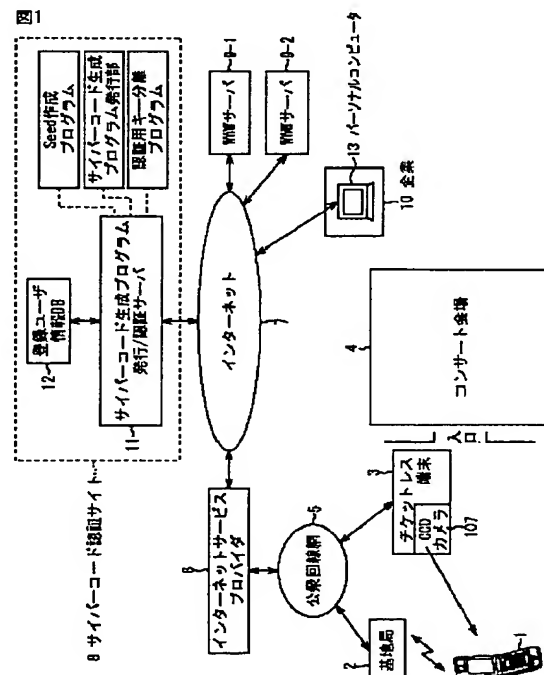
最終頁に続く

(54) 【発明の名称】 情報提供装置および方法、情報処理装置および方法、情報認証装置および方法、認証システム、記録媒体、並びにプログラム

(57) 【要約】

【課題】 プログラム自体を認証キーとして機能させるようにする。

【解決手段】 サイバーコード認証サイト 8 は、ユーザ ID、乱数および現在時刻を基に、サイバーコード生成プログラムを作成し、携帯電話機 1 に送信する。携帯電話機 1 は、受信したサイバーコード生成プログラムを実行してサイバーコードを生成し、表示させる。チケットレス端末 3 は、携帯電話機 1 に表示されているサイバーコードを CCD カメラ 107 で撮像し、認識されたコード番号をサイバーコード認証サイト 8 に送信する。サイバーコード認証サイト 8 は、コード番号に含まれるユーザ ID を基に、登録ユーザ情報 DB 12 から乱数および時刻情報を検索し、再度サイバーコード生成プログラムを作成する。そして、作成されたプログラムを実行することにより得られるサイバーコードのコード番号から、ユーザが認証される。



【特許請求の範囲】

【請求項 1】 情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行手段と、前記発行手段により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発生する乱数発生手段と、前記乱数発生手段により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、所定画像を生成するための前記プログラムを作成する作成手段と、前記作成手段により作成された前記プログラムを前記情報処理装置に提供する提供手段とを備えることを特徴とする情報提供装置。

【請求項 2】 前記ユーザIDに対応付けて、前記乱数および前記受信時刻を記録する記録手段をさらに備えることを特徴とする請求項 1 に記載の情報提供装置。

【請求項 3】 前記所定画像は、2 次元コードであることを特徴とする請求項 1 に記載の情報提供装置。

【請求項 4】 情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行処理ステップと、前記発行処理ステップの処理により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、前記乱数発生処理ステップの処理により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、所定画像を生成するための前記プログラムを作成する作成処理ステップと、前記作成処理ステップの処理により作成された前記プログラムを前記情報処理装置に提供する提供処理ステップとを含むことを特徴とする情報提供方法。

【請求項 5】 情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行処理ステップと、前記発行処理ステップの処理により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、前記乱数発生処理ステップの処理により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、所定画像を生成するための前記プログラムを作成する作成処理ステップと、前記作成処理ステップの処理により作成された前記プログラムを前記情報処理装置に提供する提供処理ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 6】 情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行処理ステップと、前記発行処理ステップの処理により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発

生する乱数発生処理ステップと、

前記乱数発生処理ステップの処理により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、所定画像を生成するための前記プログラムを作成する作成処理ステップと、

前記作成処理ステップの処理により作成された前記プログラムを前記情報処理装置に提供する提供処理ステップとをコンピュータに実行させるプログラム。

【請求項 7】 情報提供装置から提供されるプログラムを取得する情報処理装置において、前記情報提供装置に対して前記プログラムの送信を要求する要求手段と、前記要求手段に基づいて前記情報提供装置から提供される前記プログラムを受信する受信手段と、前記受信手段により受信された前記プログラムを実行し、所定画像を生成する生成手段と、前記生成手段により生成された前記所定画像を表示する表示手段とを備えることを特徴とする情報処理装置。

【請求項 8】 前記生成手段は、前記プログラムの実行時刻を基に、前記所定画像を生成することを特徴とする請求項 7 に記載の情報処理装置。

【請求項 9】 前記生成手段は、所定時間毎に前記所定画像を生成し、前記表示手段は、前記生成手段により所定時間毎に生成される前記所定画像を表示することを特徴とする請求項 7 に記載の情報処理装置。

【請求項 10】 前記所定画像は、2 次元コードであり、前記 2 次元コードには、ユーザIDを示すコード情報が含まれていることを特徴とする請求項 7 に記載の情報処理装置。

【請求項 11】 情報提供装置から提供されるプログラムを取得する情報処理装置の情報処理方法において、前記情報提供装置に対して前記プログラムの送信を要求する要求処理ステップと、前記要求処理ステップの処理に基づいて前記情報提供装置から提供される前記プログラムを受信する受信処理ステップと、前記受信処理ステップの処理により受信された前記プログラムを実行し、所定画像を生成する生成処理ステップと、前記生成処理ステップの処理により生成された前記所定画像を表示する表示処理ステップとを含むことを特徴とする情報処理方法。

【請求項 12】 情報提供装置から提供されるプログラムを取得する情報処理装置を制御するプログラムであって、前記情報提供装置に対して前記プログラムの送信を要求する要求処理ステップと、

前記要求処理ステップの処理に基づいて前記情報提供装

置から提供される前記プログラムを受信する受信処理ステップと、
前記受信処理ステップの処理により受信された前記プログラムを実行し、所定画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記所定画像を表示する表示処理ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 1 3】 情報提供装置から提供されるプログラムを取得する情報処理装置を制御するコンピュータに、前記情報提供装置に対して前記プログラムの送信を要求する要求処理ステップと、
前記要求処理ステップの処理に基づいて前記情報提供装置から提供される前記プログラムを受信する受信処理ステップと、
前記受信処理ステップの処理により受信された前記プログラムを実行し、所定画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記所定画像を表示する表示処理ステップとを実行させるプログラム。

【請求項 1 4】 他の装置に記録されているユーザ情報を取得することが可能な情報認証装置において、
第 1 の画像を撮像する撮像手段と、
前記撮像手段により撮像された前記第 1 の画像に対応する第 1 の情報を認識する認識手段と、
前記認識手段により認識された前記第 1 の情報に含まれるユーザIDを基に、前記他の装置に記録されている前記ユーザ情報を検索する検索手段と、
前記検索手段により検索された前記ユーザ情報を基に、第 2 の画像を生成するためのプログラムを作成する作成手段と、
前記作成手段により作成された前記プログラムを実行し、前記第 2 の画像を生成する生成手段と、
前記生成手段により生成された前記第 2 の画像に対応する第 2 の情報と、前記認識手段により認識された前記第 1 の情報を認証する認証手段とを備えることを特徴とする情報認証装置。

【請求項 1 5】 前記撮像手段は、情報処理装置の表示部に表示されている前記第 1 の画像を撮像することを特徴とする請求項 1 4 に記載の情報認証装置。

【請求項 1 6】 前記ユーザ情報は、少なくとも乱数および時刻情報を含み、
前記検索手段は、前記ユーザIDを基に、前記乱数および前記時刻情報を検索し、
前記作成手段は、前記検索手段により検索された前記乱数および前記時刻情報、並びに前記ユーザIDを基に、前記第 2 の画像を生成するための前記プログラムを作成することを特徴とする請求項 1 4 に記載の情報認証装置。

【請求項 1 7】 前記生成手段は、前記プログラムの実行時刻を基に、前記第 2 の画像を生成することを特徴とする請求項 1 4 に記載の情報認証装置。

【請求項 1 8】 前記第 1 の画像および前記第 2 の画像は、2 次元コードであり、
前記第 1 の情報および前記第 2 の情報は、コード番号を示す情報であることを特徴とする請求項 1 4 に記載の情報認証装置。

【請求項 1 9】 他の装置に記録されているユーザ情報を取得することが可能な情報認証装置の情報認証方法において、

第 1 の画像を撮像する撮像処理ステップと、
前記撮像処理ステップの処理により撮像された前記第 1 の画像に対応する第 1 の情報を認識する認識処理ステップと、
前記認識処理ステップの処理により認識された前記第 1 の情報に含まれるユーザIDを基に、前記他の装置に記録されている前記ユーザ情報を検索する検索処理ステップと、
前記検索処理ステップの処理により検索された前記ユーザ情報を基に、第 2 の画像を生成するためのプログラムを作成する作成処理ステップと、
前記作成処理ステップの処理により作成された前記プログラムを実行し、前記第 2 の画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記第 2 の画像に対応する第 2 の情報と、前記認識処理ステップの処理により認識された前記第 1 の情報を認証する認証処理ステップとを含むことを特徴とする情報認証方法。

【請求項 2 0】 他の装置に記録されているユーザ情報を取得することが可能な情報認証装置を制御するプログラムであって、

第 1 の画像を撮像する撮像処理ステップと、
前記撮像処理ステップの処理により撮像された前記第 1 の画像に対応する第 1 の情報を認識する認識処理ステップと、
前記認識処理ステップの処理により認識された前記第 1 の情報に含まれるユーザIDを基に、前記他の装置に記録されている前記ユーザ情報を検索する検索処理ステップと、
前記検索処理ステップの処理により検索された前記ユーザ情報を基に、第 2 の画像を生成するためのプログラムを作成する作成処理ステップと、
前記作成処理ステップの処理により作成された前記プログラムを実行し、前記第 2 の画像を生成する生成処理ステップと、
前記生成処理ステップの処理により生成された前記第 2 の画像に対応する第 2 の情報と、前記認識処理ステップの処理により認識された前記第 1 の情報を認証する認証処理ステップとを含むことを特徴とするコンピュータが

読み取り可能なプログラムが記録されている記録媒体。

【請求項 2 1】 他の装置に記録されているユーザ情報を取得することが可能な情報認証装置を制御するコンピュータに、

第 1 の画像を撮像する撮像処理ステップと、

前記撮像処理ステップの処理により撮像された前記第 1 の画像に対応する第 1 の情報を認識する認識処理ステップと、

前記認識処理ステップの処理により認識された前記第 1 の情報に含まれるユーザIDを基に、前記他の装置に記録されている前記ユーザ情報を検索する検索処理ステップと、

前記検索処理ステップの処理により検索された前記ユーザ情報を基に、第 2 の画像を生成するためのプログラムを作成する作成処理ステップと、

前記作成処理ステップの処理により作成された前記プログラムを実行し、前記第 2 の画像を生成する生成処理ステップと、

前記生成処理ステップの処理により生成された前記第 2 の画像に対応する第 2 の情報と、前記認識処理ステップの処理により認識された前記第 1 の情報を認証する認証処理ステップとを実行させるプログラム。

【請求項 2 2】 情報提供装置、情報処理装置および情報認証装置からなる認証システムにおいて、

前記情報提供装置は、

前記情報処理装置から送信されてくるプログラムの発行要求を受けて、前記情報処理装置に対して、ユーザIDを発行する発行手段と、

前記発行手段により発行された前記ユーザID、および前記発行要求の受信時刻を基に、乱数を発生する乱数発生手段と、

前記乱数発生手段により発生された前記乱数、前記ユーザID、および前記受信時刻を基に、第 1 の画像を生成するための第 1 のプログラムを作成する第 1 の作成手段と、

前記第 1 の作成手段により作成された前記第 1 のプログラムを前記情報処理装置に提供する提供手段と、

前記ユーザIDに対応付けて、前記乱数および前記受信時刻を記録する記録手段とを備え、

前記情報処理装置は、

前記情報提供装置に対して前記第 1 のプログラムの送信を要求する要求手段と、

前記情報提供装置から提供される前記第 1 のプログラムを受信する受信手段と、

前記受信手段により受信された前記第 1 のプログラムを実行し、前記第 1 の画像を生成する第 1 の生成手段と、

前記第 1 の生成手段により生成された前記第 1 の画像を表示する表示手段とを備え、

前記情報認証装置は、

前記情報処理装置の前記表示手段に表示されている前記

第 1 の画像を撮像する撮像手段と、

前記撮像手段により撮像された前記第 1 の画像に対応する第 1 の情報を認識する認識手段と、

前記認識手段により認識された前記第 1 の情報に含まれる前記ユーザIDを基に、前記情報提供装置の前記記録手段に記録されている前記乱数および前記受信時刻を検索する検索手段と、

前記検索手段により検索された前記乱数および前記受信時刻を基に、第 2 の画像を生成するための第 2 のプログラムを作成する第 2 の作成手段と、

前記第 2 の作成手段により作成された前記第 2 のプログラムを実行し、前記第 2 の画像を生成する第 2 の生成手段と、

前記第 2 の生成手段により生成された前記第 2 の画像に対応する第 2 の情報と、前記認識手段により認識された前記第 1 の情報を認証する認証手段とを備えることを特徴とする認証システム。

【請求項 2 3】 前記第 1 の生成手段は、前記第 1 のプログラムの実行時刻を基に、前記第 1 の画像を生成し、前記第 2 の生成手段は、前記第 2 のプログラムの実行時刻を基に、前記第 2 の画像を生成することを特徴とする請求項 2 2 に記載の認証システム。

【請求項 2 4】 前記第 1 の画像および前記第 2 の画像は、2 次元コードであることを特徴とする請求項 2 2 に記載の認証システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】本発明は、情報提供装置および方法、情報処理装置および方法、情報認証装置および方法、認証システム、記録媒体、並びにプログラムに関し、特に、2 次元コードを生成するためのプログラムを認証キーとして利用するようにした情報提供装置および方法、情報処理装置および方法、情報認証装置および方法、認証システム、記録媒体、並びにプログラムに関する。

【0 0 0 2】

【従来の技術】従来から、物品の種類や状態などを示す英数字をバーコード化し、例えば、物品に添付しておき、その添付されたバーコードを読み取って、物品の種類や状態などの情報を取得するバーコードシステムが、多くの産業分野に普及している。

【0 0 0 3】このようなバーコードは 1 次元バーコードと呼ばれ、太さの異なるバー（黒色の棒状部分）とスペース（空白部分）の組み合わせで所定のコードが示され、このコードパターンから読み出されるコード番号に基づいて、物品を識別し管理するようになされている。

【0 0 0 4】また、より多くの情報量をコード化するために、複数の方形セルを所定の配列規則に従って 2 次元的に配置させるような 2 次元コードも提案されている。

2 次元コードのコードパターンから読み出されるコード

番号は、固有（唯一）の番号であるため、特定のユーザを認証するための認証キーとして利用することも可能である。

【0005】例えば、コンサートの開催主が、コンサート会場に入場しようとするユーザに対して、認証キーとなる２次元コードを配布するなどの利用方法が考えられる。この場合、コンサートの開催主は、コンサートの入場チケットを購入したユーザに対して、固有のコード番号を割り当てる。そして、開催主は、２次元コードを生成するためのプログラムを実行し、コード番号を入力することによって、所定の２次元コードを生成し、認証キーとしてユーザに配布する。２次元コードが配布されたユーザは、コンサート会場にて、そのコードを提示して、所定の認識端末にて認証されると、入場が許可される。

【0006】

【発明が解決しようとする課題】しかしながら、上述したプログラムは、入力されたコード番号を意味する２次元コードを生成するものであるため、コード番号さえわかれば、第三者によって、不正に同一の２次元コードが生成され、利用されてしまう恐れがあった。

【0007】また、２次元コードが印刷された媒体もしくは２次元コードの画像データが第三者の手に渡ってしまうと、いわゆる「なりすまし」が可能になってしまう課題があった。

【0008】本発明はこのような状況に鑑みてなされたものであり、２次元コードを生成するためのプログラム自体をユーザ毎に変化させて、それを認証キーとして機能させ、そのプログラムを所有するユーザのみが所定の２次元コードを作成することにより、高精度にユーザ認証することができるようにするものである。

【0009】

【課題を解決するための手段】本発明の情報提供装置は、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行手段と、発行手段により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生手段と、乱数発生手段により発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成する作成手段と、作成手段により作成されたプログラムを情報処理装置に提供する提供手段とを備えることを特徴とする。

【0010】ユーザIDに対応付けて、乱数および受信時刻を記録する記録手段をさらに設けるようにすることができる。

【0011】所定画像は、２次元コードであるものとすることができる。

【0012】本発明の情報提供方法は、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行処理ステッ

ブと、発行処理ステップの処理により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、乱数発生処理ステップの処理により発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを情報処理装置に提供する提供処理ステップとを含むことを特徴とする。

【0013】本発明の第１の記録媒体に記録されているプログラムは、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行処理ステップと、発行処理ステップの処理により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、乱数発生処理ステップの処理により発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを情報処理装置に提供する提供処理ステップとを含むことを特徴とする。

【0014】本発明の第１のプログラムは、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行処理ステップと、発行処理ステップの処理により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生処理ステップと、乱数発生処理ステップの処理により発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを情報処理装置に提供する提供処理ステップとをコンピュータに実行させることを特徴とする。

【0015】本発明の情報提供装置および方法、並びに第１のプログラムにおいては、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDが発行され、発行されたユーザID、および発行要求の受信時刻を基に、乱数が発生され、発生された乱数、ユーザID、および受信時刻を基に、所定画像を生成するためのプログラムが作成され、作成されたプログラムが情報処理装置に提供される。

【0016】本発明の情報処理装置は、情報提供装置に対してプログラムの送信を要求する要求手段と、要求手段に基づいて情報提供装置から提供されるプログラムを受信する受信手段と、受信手段により受信されたプログラムを実行し、所定画像を生成する生成手段と、生成手段により生成された所定画像を表示する表示手段とを備えることを特徴とする。

【0017】生成手段には、プログラムの実行時刻を基に、所定画像を生成させることができる。

【0018】生成手段には、所定時間毎に所定画像を生

成させるようにし、表示手段には、生成手段により所定時間毎に生成される所定画像を表示させることができる。

【0019】所定画像は、2次元コードであるものとすることができ、2次元コードには、ユーザIDを示すコード情報が含まれているものとすることができ。

【0020】本発明の情報処理方法は、情報提供装置に対してプログラムの送信を要求する要求処理ステップと、要求処理ステップの処理に基づいて情報提供装置から提供されるプログラムを受信する受信処理ステップと、受信処理ステップの処理により受信されたプログラムを実行し、所定画像を生成する生成処理ステップと、生成処理ステップの処理により生成された所定画像を表示する表示処理ステップとを含むことを特徴とする。

【0021】本発明の第2の記録媒体に記録されているプログラムは、情報提供装置に対してプログラムの送信を要求する要求処理ステップと、要求処理ステップの処理に基づいて情報提供装置から提供されるプログラムを受信する受信処理ステップと、受信処理ステップの処理により受信されたプログラムを実行し、所定画像を生成する生成処理ステップと、生成処理ステップの処理により生成された所定画像を表示する表示処理ステップとを含むことを特徴とする。

【0022】本発明の第2のプログラムは、情報提供装置に対してプログラムの送信を要求する要求処理ステップと、要求処理ステップの処理に基づいて情報提供装置から提供されるプログラムを受信する受信処理ステップと、受信処理ステップの処理により受信されたプログラムを実行し、所定画像を生成する生成処理ステップと、生成処理ステップの処理により生成された所定画像を表示する表示処理ステップとをコンピュータに実行させることを特徴とする。

【0023】本発明の情報処理装置および方法、並びに第2のプログラムにおいては、情報提供装置に対してプログラムの送信が要求され、情報提供装置から提供されるプログラムが受信され、受信されたプログラムが実行されて所定画像が生成され、生成された所定画像が表示される。

【0024】本発明の情報認証装置は、第1の画像を撮像する撮像手段と、撮像手段により撮像された第1の画像に対応する第1の情報を認識する認識手段と、認識手段により認識された第1の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報を検索する検索手段と、検索手段により検索されたユーザ情報を基に、第2の画像を生成するためのプログラムを作成する作成手段と、作成手段により作成されたプログラムを実行し、第2の画像を生成する生成手段と、生成手段により生成された第2の画像に対応する第2の情報と、認識手段により認識された第1の情報を認証する認証手段とを備えることを特徴とする。

【0025】撮像手段には、情報処理装置の表示部に表示されている第1の画像を撮像させることができる。

【0026】ユーザ情報は、少なくとも乱数および時刻情報を含むようにすることができ、検索手段には、ユーザIDを基に、乱数および時刻情報を検索させ、作成手段には、検索手段により検索された乱数および時刻情報、並びにユーザIDを基に、第2の画像を生成するためのプログラムを作成させることができる。

【0027】生成手段には、プログラムの実行時刻を基に、第2の画像を生成させることができる。

【0028】第1の画像および第2の画像は、2次元コードであるものとすることができ、第1の情報および第2の情報は、コード番号を示す情報であるものとすることができ。

【0029】本発明の情報認証方法は、第1の画像を撮像する撮像処理ステップと、撮像処理ステップの処理により撮像された第1の画像に対応する第1の情報を認識する認識処理ステップと、認識処理ステップの処理により認識された第1の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報を検索する検索処理ステップと、検索処理ステップの処理により検索されたユーザ情報を基に、第2の画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを実行し、第2の画像を生成する生成処理ステップと、生成処理ステップの処理により生成された第2の画像に対応する第2の情報と、認識処理ステップの処理により認識された第1の情報を認証する認証処理ステップとを含むことを特徴とする。

【0030】本発明の第3の記録媒体に記録されているプログラムは、第1の画像を撮像する撮像処理ステップと、撮像処理ステップの処理により撮像された第1の画像に対応する第1の情報を認識する認識処理ステップと、認識処理ステップの処理により認識された第1の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報を検索する検索処理ステップと、検索処理ステップの処理により検索されたユーザ情報を基に、第2の画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを実行し、第2の画像を生成する生成処理ステップと、生成処理ステップの処理により生成された第2の画像に対応する第2の情報と、認識処理ステップの処理により認識された第1の情報を認証する認証処理ステップとを含むことを特徴とする。

【0031】本発明の第3のプログラムは、第1の画像を撮像する撮像処理ステップと、撮像処理ステップの処理により撮像された第1の画像に対応する第1の情報を認識する認識処理ステップと、認識処理ステップの処理により認識された第1の情報に含まれるユーザIDを基

に、他の装置に記録されているユーザ情報を検索する検

索処理ステップと、検索処理ステップの処理により検索されたユーザ情報を基に、第 2 の画像を生成するためのプログラムを作成する作成処理ステップと、作成処理ステップの処理により作成されたプログラムを実行し、第 2 の画像を生成する生成処理ステップと、生成処理ステップの処理により生成された第 2 の画像に対応する第 2 の情報と、認識処理ステップの処理により認識された第 1 の情報を認証する認証処理ステップとをコンピュータに実行させることを特徴とする。

【0 0 3 2】本発明の情報認証装置および方法、並びに第 3 のプログラムにおいては、第 1 の画像が撮像され、撮像された第 1 の画像に対応する第 1 の情報が認識され、認識された第 1 の情報に含まれるユーザIDを基に、他の装置に記録されているユーザ情報が検索され、検索されたユーザ情報を基に、第 2 の画像を生成するためのプログラムが作成され、作成されたプログラムが実行されて第 2 の画像が生成され、生成された第 2 の画像に対応する第 2 の情報と、認識された第 1 の情報が認証される。

【0 0 3 3】本発明の認証システムは、情報提供装置が、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDを発行する発行手段と、発行手段により発行されたユーザID、および発行要求の受信時刻を基に、乱数を発生する乱数発生手段と、乱数発生手段により発生された乱数、ユーザID、および受信時刻を基に、第 1 の画像を生成するための第 1 のプログラムを作成する第 1 の作成手段と、第 1 の作成手段により作成された第 1 のプログラムを情報処理装置に提供する提供手段と、ユーザIDに対応付けて、乱数および受信時刻を記録する記録手段とを備え、情報処理装置が、情報提供装置に対して第 1 のプログラムの送信を要求する要求手段と、情報提供装置から提供される第 1 のプログラムを受信する受信手段と、受信手段により受信された第 1 のプログラムを実行し、第 1 の画像を生成する第 1 の生成手段と、第 1 の生成手段により生成された第 1 の画像を表示する表示手段とを備え、情報認証装置が、情報処理装置の表示手段に表示されている第 1 の画像を撮像する撮像手段と、撮像手段により撮像された第 1 の画像に対応する第 1 の情報を認識する認識手段と、認識手段により認識された第 1 の情報に含まれるユーザIDを基に、情報提供装置の記録手段に記録されている乱数および受信時刻を検索する検索手段と、検索手段により検索された乱数および受信時刻を基に、第 2 の画像を生成するための第 2 のプログラムを作成する第 2 の作成手段と、第 2 の作成手段により作成された第 2 のプログラムを実行し、第 2 の画像を生成する第 2 の生成手段と、第 2 の生成手段により生成された第 2 の画像に対応する第 2 の情報と、認識手段により認識された第 1 の情報を認証する認証手段とを備えることを特徴とする。

【0 0 3 4】第 1 の生成手段には、第 1 のプログラムの実行時刻を基に、第 1 の画像を生成させ、第 2 の生成手段には、第 2 のプログラムの実行時刻を基に、第 2 の画像を生成させることができる。

【0 0 3 5】第 1 の画像および第 2 の画像は、2 次元コードであるものとすることができる。

【0 0 3 6】本発明の認証システムにおいては、情報提供装置で、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザIDが発行され、発行されたユーザID、および発行要求の受信時刻を基に、乱数が発生され、発生された乱数、ユーザID、および受信時刻を基に、第 1 の画像を生成するための第 1 のプログラムが作成され、作成された第 1 のプログラムが情報処理装置に提供され、ユーザIDに対応付けて、乱数および受信時刻が記録され、情報処理装置で、情報提供装置に対して第 1 のプログラムの送信が要求され、情報提供装置から提供される第 1 のプログラムが受信され、受信された第 1 のプログラムが実行されて第 1 の画像が生成され、生成された第 1 の画像が表示され、情報認証装置で、情報処理装置に表示されている第 1 の画像が撮像され、撮像された第 1 の画像に対応する第 1 の情報が認識され、認識された第 1 の情報に含まれるユーザIDを基に、情報提供装置に記録されている乱数および受信時刻が検索され、検索された乱数および受信時刻を基に、第 2 の画像を生成するための第 2 のプログラムが作成され、作成された第 2 のプログラムが実行されて第 2 の画像が生成され、生成された第 2 の画像に対応する第 2 の情報と、認識された第 1 の情報が認証される。

【0 0 3 7】

【発明の実施の形態】以下、図を参照して、本発明の実施の形態について説明する。

【0 0 3 8】図 1 は、本発明を適用したチケットレスシステムの一実施の形態の構成例を示す図である。

【0 0 3 9】カメラ付デジタル携帯電話機 1（以下、単に携帯電話機 1 と称する）は、通信サービスの提供エリアを所望の広さに分割したセルにそれぞれ配置されている、固定無線端末である基地局 2 を介して、公衆回線網 5 に接続されている。

【0 0 4 0】基地局 2 は、移動無線端末である携帯電話機 1 を、例えば、W-CDMA（Wideband-Code Division Multiple Access）と呼ばれる符号分割多元接続により無線接続し、携帯電話機 1 と、2GHz の周波数帯域を利用して最大 2Mbps のデータ転送速度で大容量データを高速にデータ通信できる。

【0 0 4 1】また、基地局 2 は、有線回線を介して、公衆回線網 5 に接続されている。公衆回線網 5 は、インターネットサービスプロバイダ 6 を介してインターネット 7 に接続されているほか、図示せぬ加入者有線端末装置、コンピュータネットワーク、および企業内ネットワ

ーク等に接続されている。

【0042】携帯電話機1は、基地局2とW-CDMA方式により大容量データを高速にデータ通信できるので、電子メールの送受信、簡易ホームページの閲覧、画像の送受信等の多種に及ぶデータ通信を実行することができる。

【0043】携帯電話機1はまた、i-アプリ（登録商標）機能を有しており、サイバーコード認証サイト8から提供される様々な、Java（登録商標）言語で記述されたプログラム（いわゆるJava（登録商標）アプレット）をダウンロードすることができる。

【0044】例えば、携帯電話機1は、公衆回線網5、インターネットサービスプロバイダ6、およびインターネット7を介して、サイバーコード認証サイト8に接続し、所定の2次元コードを生成するためのプログラム（Java（登録商標）アプレット）をダウンロードすることができる。携帯電話機1は、ダウンロードされたプログラムを実行して2次元コードを生成し、生成された2次元コードを液晶ディスプレイ35（図3）に表示させる。液晶ディスプレイ35に表示された2次元コードは、後述するように、コンサート会場4に入場するための入場チケットの代替（認証キー）として利用される。

【0045】本発明では、この2次元コードの一種として、本出願人によって開発されたサイバーコード（CyberCode）（登録商標）を例に挙げて説明する。

【0046】チケットレス端末3は、CCD（Charge Coupled Device）カメラ107（図7）を有するパーソナルコンピュータなどで構成され、コンサート会場4の入口付近に設けられる。チケットレス端末3は、携帯電話機1の液晶ディスプレイ35に表示されたサイバーコードをCCDカメラ107で撮像し、その結果得られるサイバーコードの画像データから、サイバーコードのコードパターンを認識し、そのコードパターンに対応した所定の処理を実行するようになっている。

【0047】例えば、チケットレス端末3は、コードパターンから得られるコード番号を、公衆回線網5乃至インターネット7を介してサイバーコード認証サイト8に送信し、ユーザ認証を行うように要求する。チケットレス端末3は、サイバーコード認証サイト8から供給される認証結果を受信し、液晶ディスプレイ109（図7）に表示させることができる。

【0048】インターネット7には、インターネットサービスプロバイダ6、サイバコード認証サイト8、WWW（World Wide Web）サーバ9-1、9-2（以下、これらのWWWサーバ9-1、9-2を個々に区別する必要がない場合、単にWWWサーバ9と称する）、および、企業10が接続されている。

【0049】サイバーコード認証サイト8は、サイバーコード生成プログラム発行／認証サーバ11および登録ユーザ情報データベース（DB）12などで構成される。サイバーコード生成プログラム発行／認証サーバ11

は、携帯電話機1のユーザから、予め、住所、氏名、および電話番号などのユーザ情報の登録を受け付けておき、それらの情報を、登録ユーザ情報データベース12に記録するようになっている。

【0050】図2は、登録ユーザ情報データベース12に記録されているユーザ情報の記録例を示す図である。同図においては、サイバーコード生成プログラムの発行要求があったユーザに割り当てられるユーザIDがユーザ情報と関連付けられて記録されるとともに、ユーザIDに対応付けてサイバーコード生成プログラムの発行開始時刻TID、および乱数発生用SeedIDが記録される。

【0051】ユーザ情報は、主に、発行されたサイバーコードを生成するためのプログラム（認証用サイバチケット）の決済を行うときなどに利用され、ユーザ情報を基に、所定のクレジット会社や銀行などに照会され、決済が実行される。

【0052】サイバーコード生成プログラム発行／認証サーバ11は、サイバーコード生成プログラムの発行を希望するユーザからユーザIDの登録を受け付けると、ユーザ毎に固有の識別子であるユーザID（UID）を発行し、ユーザ情報に対応付けて、発行されたユーザIDを登録ユーザ情報データベース12に記録させるとともに、ユーザIDを、インターネット7を介して携帯電話機1に通知（送信）するようになっている。

【0053】サイバーコード生成プログラム発行／認証サーバ11は、携帯電話機1からユーザIDを含むサイバーコード生成プログラムの送信（発行）要求を受けて、シード（Seed）作成プログラムを起動し、受信したユーザID、および現在時刻TIDから乱数発生用SeedIDを作成するようになっている。

【0054】サイバーコード生成プログラム発行／認証サーバ11は、作成された乱数発生用SeedID、ユーザID、および現在時刻TIDからサイバーコード生成プログラムを作成し、インターネット7を介して、携帯電話機1に送信した後、ユーザIDに対応付けて、サイバーコード発行開始時刻TIDおよび作成された乱数発生用SeedIDを、登録ユーザ情報データベース12に登録（記録）するようになっている。

【0055】なお、乱数発生用SeedIDは、サイバーコード（すなわちコード番号）をランダムに生成することができるように、サイバーコード生成プログラム毎に固有の値とされ、登録ユーザ情報データベース12で管理される。しかしながら、乱数発生用SeedIDが漏洩されると、セキュリティ上好ましくない場合があるため、乱数発生用SeedIDを作成するときに用いられるデータ（ユーザIDおよびサイバーコード発行開始時刻TID）のみを登録ユーザ情報データベース12で管理させるようにして、乱数発生用SeedIDの漏洩を防止するようにしてもよい。

【0056】サイバーコード生成プログラム発行／認証

サーバ 11 は、チケットレス端末 3 から送信されてくるコード番号（すなわち、携帯電話機 1 の液晶ディスプレイ 35 に表示されたサイバーコードが CCD カメラ 107 で認識され、認識されたコードパターンに対応するコード番号）を受けて、認証用キー分離プログラムを起動し、コード番号に含まれるユーザ ID を分離するようになされている。

【0057】サイバーコード生成プログラム発行／認証サーバ 11 は、分離されたユーザ ID を基に、登録ユーザ情報データベース 12 から、対応するユーザ ID の発行開始時刻 TID および乱数発生用 Seed ID を検索し、再度、サイバーコード生成プログラムを作成するようになされている。サイバーコード生成プログラム発行／認証サーバ 11 は、作成されたサイバーコード生成プログラムを実行することにより生成されるサイバーコードを基に、ユーザ認証処理を実行するようになされている。

【0058】サイバーコード生成プログラム発行／認証サーバ 11 は、インターネット 7 を介して企業 10 が有するパーソナルコンピュータ 13 と接続され、パーソナルコンピュータ 13 から認証用サイバーチケット発行の依頼を受けて、上述したようにして、特定のユーザに対してサイバーコード生成プログラムを発行したり、企業 10 に対して、課金処理を実行するようになされている。

【0059】WWWサーバ 9 は、TCP/IP (Transmission Control Protocol/Internet Protocol) のプロトコルに従って、携帯電話機 1、もしくは企業 10 が有するパーソナルコンピュータ 13 からアクセスされ、インターネット 7 を介して、各種のホームページに代表される情報を提供する。提供される情報は、例えば、HTML (HyperText Markup Language)、XML (eXtensible Markup Language)、あるいは、コンパクト HTML などのページ記述言語で記述されている。ここでは、WWWサーバ 9-1、9-2 しか図示していないが、複数の WWWサーバ 9 が接続されることは言うまでもない。

【0060】企業 10 は、例えば、コンサート会場 4 で開催されるコンサートの開催主である。企業 10 は、パーソナルコンピュータ 13 を用いて、インターネット 7 を介して、サイバーコード認証サイト 8 に認証用サイバーチケットの発行およびユーザ認証を依頼したり、チケット発行の費用の請求を受ける。企業 10 はまた、ネットワークを介さずに、その他の方法を用いて（すなわち、オフラインで）、サイバーコード認証サイト 8 に認証用サイバーチケットの発行およびユーザ認証を依頼したり、チケット発行の費用の請求を受けるようにしてもよい。

【0061】図 3 は、携帯電話機 1 の外観の構成例を示す図である。同図に示されるように、携帯電話機 1 は、表示部 22 および本体 23 で構成され、中央のヒンジ部 21 により折り畳み可能に形成されている。

【0062】表示部 22 は、上端左部に引出しまたは収納可能な送受信用のアンテナ 31 を有する。携帯電話機 1 は、アンテナ 31 を介して、固定無線局である基地局 2 との間で電波を送受信する。

【0063】また、表示部 22 は、上端中央部にほぼ 180 度の角度範囲で回転自在なカメラ部 32 を有する。携帯電話機 1 は、カメラ部 32 の CCD カメラ 33 によって所望の撮像対象を撮像する。

【0064】カメラ部 32 が使用者によってほぼ 180 度回転されて位置決めされた場合、図 4 に示すように、表示部 22 は、カメラ部 32 の背面側中央に設けられたスピーカ 34 が正面側に位置する状態となる。これにより、携帯電話機 1 は、通常の音声通話状態に切り換わる。

【0065】さらに、表示部 22 の正面に液晶ディスプレイ 35 が設けられている。液晶ディスプレイ 35 は、電波の受信状態、電池残量、電話帳として登録されている相手先名や電話番号および発信履歴等の他、電子メールの内容、簡易ホームページ、カメラ部 32 の CCD カメラ 33 で撮像した画像などを表示する。

【0066】一方、本体 23 には、その表面に「0」乃至「9」の数字キー、発呼キー、リダイヤルキー、終話及び電源キー、クリアキー及び電子メールキー等の操作キー 41 が設けられている。操作キー 41 の操作に対応した各種指示が、携帯電話機 1 に入力される。

【0067】また、本体 23 の操作キー 41 の下部にメモボタン 42 およびマイクロフォン 43 が設けられている。携帯電話機 1 は、メモボタン 42 が操作されたとき、通話中の相手の音声を録音する。携帯電話機 1 は、マイクロフォン 43 によって通話時の使用者の音声を録音する。

【0068】さらに、本体 23 の操作キー 41 の上部に回転自在なジョグダイヤル 44 が、本体 23 の表面から僅かに突出した状態で設けられている。携帯電話機 1 は、ジョグダイヤル 44 に対する回転操作に応じて、液晶ディスプレイ 35 に表示されている電話帳リストもしくは電子メールのスクロール動作、簡易ホームページのページ捲り動作、または画像の送り動作等の種々の動作を実行する。

【0069】例えば、本体 23 は、使用者によるジョグダイヤル 44 の回転操作に応じて液晶ディスプレイ 35 に表示された電話帳リストの複数の電話番号の中から所望の電話番号を選択し、ジョグダイヤル 44 が本体 23 の内部方向に押圧されたとき、選択されている電話番号を確定して、確定した電話番号に対して自動的に発呼処理を行う。

【0070】なお、本体 23 は、背面側に図示せぬバッテリーバックが装着されており、終話／電源キーがオン状態になると、バッテリーバックから各回路部に対して電力が供給されて動作可能な状態に起動する。

【0071】ところで、本体23の左側面上部に抜差自在なメモリカード51を装着するためのメモリカードスロット45が設けられている。携帯電話機1は、メモボタン42が押下されると、通話中の相手の音声を装着されているメモリカード51に記録する。携帯電話機1は、使用者の操作に応じて、電子メール、簡易ホームページ、CCDカメラ33で撮像した画像を、装着されているメモリカード51に記録する。

【0072】同図に示されるメモリカード51は、例えば、メモリスティック（商標）と呼ばれる本出願人によって開発されたフラッシュメモリカードの一種である。このメモリカード51は、縦21.5×横50×厚さ2.8[mm]の小型薄型形状のプラスチックケース内に電気的に書換えや消去が可能な不揮発性メモリであるEEPROM（Electrically Erasable and Programmable Read Only Memory）の一種であるフラッシュメモリ素子を格納したものであり、10ピン端子を介して画像や音声、音楽等の各種データの書き込みおよび読み出しが可能となっている。

【0073】またメモリカード51は、大容量化等による内蔵フラッシュメモリの仕様変更に対しても、使用する機器で互換性を確保することができる独自のシリアルプロトコルを採用し、最大書込速度1.5[MB/S]、最大読出速度2.45[MB/S]の高速性能を実現しているとともに、誤消去防止スイッチを設けて高い信頼性を確保している。

【0074】従って、携帯電話機1は、このようなメモリカード51を装着可能に構成されているために、メモリカード51を介して、他の電子機器との間でデータの共有化を図ることができる。

【0075】図5に示すように、携帯電話機1は、表示部22および本体23の各部を統括的に制御する主制御部61に対して、電源回路部65、操作入力制御部62、画像エンコーダ63、カメラインターフェース（I/F）部64、LCD（Liquid Crystal Display）制御部66、画像デコーダ67、多重分離部68、記憶再生部73、変復調回路部69、および音声コーデック70がメインバス71を介して互いに接続されるとともに、画像エンコーダ63、画像デコーダ67、多重分離部68、変復調回路部69、および音声コーデック70が同期バス72を介して互いに接続されて構成されている。

【0076】電源回路部65は、使用者の操作により終話／電源キーがオン状態にされると、バッテリーパックから各部に対して電力を供給することにより、携帯電話機1を動作可能な状態に起動する。

【0077】携帯電話機1は、CPU（Central Processing Unit）、ROM（Read Only Memory）およびRAM（Random Access Memory）等である主制御部61の制御に基づいて、音声通話モードにおいて、マイクロフォン43で集音した音声信号を音声コーデック70によってデジタル

音声データに変換する。携帯電話機1は、デジタル音声データを変復調回路部69でスペクトラム拡散処理し、送受信回路部74でデジタルアナログ変換処理および周波数変換処理を施した後にアンテナ31を介して送信する。

【0078】また、携帯電話機1は、音声通話モードにおいて、アンテナ31で受信した受信信号を増幅して周波数変換処理およびアナログデジタル変換処理を施し、変復調回路部69でスペクトラム逆拡散処理し、音声コーデック70によってアナログ音声信号に変換する。携帯電話機1は、アナログ音声信号に対応する音声をスピーカ34に出力させる。

【0079】さらに、携帯電話機1は、データ通信モードにおいて、電子メールを送信する場合、操作キー41およびジョグダイヤル44の操作によって入力された電子メールのテキストデータを操作入力制御部62を介して主制御部61に送出する。

【0080】主制御部61は、テキストデータを変復調回路部69でスペクトラム拡散処理し、送受信回路部74でデジタルアナログ変換処理および周波数変換処理を施した後にアンテナ31を介して基地局2へ送信する。

【0081】これに対して携帯電話機1は、データ通信モードにおいて、電子メールを受信する場合、アンテナ31を介して基地局2から受信した受信信号を変復調回路部69でスペクトラム逆拡散処理して、元のテキストデータを復元した後、LCD制御部66を介して液晶ディスプレイ35に電子メールとして表示する。

【0082】この後、携帯電話機1は、使用者の操作に応じて受信した電子メールを、記憶再生部73を介してメモリカード51に記録することも可能である。

【0083】携帯電話機1は、データ通信モードにおいて画像データを送信する場合、CCDカメラ33で撮像された画像データを、カメラインターフェース部64を介して画像エンコーダ63に供給する。

【0084】因みに携帯電話機1は、画像データを送信しない場合には、CCDカメラ33で撮像した画像データを、カメラインターフェース部64およびLCD制御部66を介して液晶ディスプレイ35に直接表示することも可能である。

【0085】画像エンコーダ63は、CCDカメラ33から供給された画像データを、例えば、MPEG（Moving Picture Experts Group）2またはMPEG4等の所定の符号化方式によって圧縮符号化することにより符号化画像データに変換し、これを多重分離部68に送出する。

【0086】このとき同時に携帯電話機1は、CCDカメラ33で撮像中にマイクロフォン43で集音した音声を、音声コーデック70を介してデジタルの音声データとして多重分離部68に送出する。

【0087】多重分離部68は、画像エンコーダ63から供給された符号化画像データと音声コーデック70か

ら供給された音声データとを所定の方式で多重化し、その結果得られる多重化データを変復調回路部 69 でスペクトラム拡散処理し、送受信回路部 74 でデジタルアナログ変換処理および周波数変換処理を施した後にアンテナ 31 を介して送信する。

【0088】これに対して携帯電話機 1 は、データ通信モードにおいて、例えば、簡易ホームページ等にリンクされた動画像ファイルのデータを受信する場合、アンテナ 31 を介して基地局 2 から受信した受信信号を変復調回路部 69 でスペクトラム逆拡散処理し、その結果得られる多重化データを多重分離部 68 に送出する。

【0089】多重分離部 68 は、多重化データを符号化画像データと音声データとに分離し、同期バス 72 を介して、符号化画像データを画像デコーダ 67 に供給するとともに、音声データを音声コーデック 70 に供給する。

【0090】画像デコーダ 67 は、符号化画像データを MPEG2 または MPEG4 等の所定の符号化方式に対応した復号方式でデコードすることにより再生動画像データを生成し、これを LCD 制御部 66 を介して液晶ディスプレイ 35 に供給する。これにより、携帯電話機 1 は、例えば、簡易ホームページにリンクされた動画像ファイルに含まれる動画データを表示する。

【0091】このとき同時に音声コーデック 70 は、音声データをアナログ音声信号に変換した後、これをスピーカ 34 に供給する。これにより、携帯電話機 1 は、例えば、簡易ホームページにリンクされた動画像ファイルに含まれる音声データを再生する。

【0092】この場合も電子メールの場合と同様に、携帯電話機 1 は、受信した簡易ホームページ等にリンクされたデータを使用者の操作により記憶再生部 73 を介してメモリカード 51 に記録することが可能である。

【0093】図 6 は、携帯電話機 1 の機能を説明するブロック図である。

【0094】出力制御プログラム 81 は、操作キー 41 もしくはジョグダイヤル 44 を用いて、ユーザが入力した操作または命令を示す信号を、対応するアプリケーションに供給したり、各種アプリケーションの処理に基づいて、マイクロフォン 43 から入力されたユーザの音声データなどをスピーカ 34 に出力して音声を再生させたり、CCD カメラ 33 で撮像された画像データなどを液晶ディスプレイ 35 に出力して画像を表示させたり、所定のデータをメモリカード 51 に供給してそこに記録させたり、所定のデータを、データ通信プログラム 87 を介してアンテナ 31 に出力して対応する電波を出力させる処理を制御するプログラムである。

【0095】ウェブブラウザ 82 は、WWW サーバ 9 の情報をクライアント側でブラウズするためのソフトウェアプログラムである。WWW サーバ 9 と WWW クライアント間で、所定の通信プロトコルに基づいて通信を実行し、さ

らにセキュリティ機能や音声／動画などのマルチメディアデータの再生、WWW サーバ 9 と WWW クライアントとの間でプログラム転送を可能にする拡張言語（例えば、Java（登録商標））などをサポートするものである。

【0096】表示プログラム 83 は、メモリカード 51 に記録されている画像データもしくは CCD カメラ 33 で撮像された画像データを、入出力制御プログラム 81 の処理により液晶ディスプレイ 35 に表示させるために、データを変換したり、画像処理を実行するためのプログラムである。

【0097】電子メールプログラム 84 は、インターネットサービスプロバイダ 6 に対し、自分宛の電子メールを送信するように要求し、自分宛の電子メールをダウンロード（受信）するプログラムである。電子メールプログラム 84 はまた、インターネットサービスプロバイダ 6 に対し、所定の宛先に電子メールを送信するように要求するプログラムである。

【0098】Java（登録商標）アプレット実行プログラム 85 は、サイバーコード認証サイト 8 にアクセスし、所定の Java（登録商標）アプレットをダウンロードする際に必要となるユーザ ID を登録したり、所定の Java（登録商標）アプレットをダウンロードする処理を実行するプログラムである。

【0099】Java（登録商標）アプレット実行プログラム 85 はまた、サイバーコード認証サイト 8 からダウンロードされ、メモリ 86 に記憶されている Java（登録商標）アプレット 91-1 および 91-2 の中から、ユーザの操作によっていずれかが選択されると、選択された Java（登録商標）アプレットを実行する。例えば、後述するように、Java（登録商標）アプレット（サイバーコード生成プログラム）の実行によって、認証用のサイバーコード（認証用サイバーチケット）が生成され、生成されたサイバーコードが液晶ディスプレイ 35 に表示される。

【0100】データ通信プログラム 87 は、主制御部 61 が実行しているアプリケーション（例えば、ウェブブラウザ 82）において、アンテナ 31 を介して、他の装置と情報の通信を行う場合、その通信を制御するプログラムである。

【0101】図 7 乃至図 9 は、図 1 のチケットレス端末 3 の構成例を示す図である。このチケットレス端末装置 3 は、基本的に、本体 101 と本体 101 に対して開閉自在に取り付けられた表示部 102 により構成されている。

【0102】本体 101 は、その上面に各種文字や記号および数字などを入力するとき操作される操作キー 103、マウスカーソルの移動に用いられるスティック式ポインティングデバイス（以下、適宜、スティックと称する）104、通常のマウスにおける左ボタンおよび右ボタンに相当する左クリックボタン 104A および 10

10

20

30

40

50

4 B、マウスカーソルをスクロールボタンに合わせることなくスクロールバーを操作するためのセンタボタン104 C、内蔵スピーカ105 Aおよび105 B、押圧式の電源スイッチ106、表示部102に設けられたCCDカメラ107用のシャッターボタン108、LED (Light Emitting Diode) で構成された電源ランプPL、電池ランプBLおよびメッセージランプMLなどが設けられている。

【0103】表示部102の正面には、例えば、TFT (Thin Film Transistor) カラー液晶でなる液晶ディスプレイ109が設けられており、その中央上端部にはCCDカメラ107を備えた撮像部111が表示部102に対して回動自在に設けられている。すなわち、この撮像部111は、表示部102と同一の方向と、その逆の方向(背面の方向)との間の180度の範囲の任意の位置に回動することができるようになされている。撮像部111には、調整リング112によりフォーカスの調整が可能となるようになされている。

【0104】また表示部102は、撮像部111の左端近傍における正面側および背面側にマイクロフォン113が設けられており、マイクロフォン113を介して表示部102の正面側から背面側までの広範囲に渡って集音するようになされている。

【0105】さらに表示部102は、液晶ディスプレイ109の左端近傍および右端近傍にそれぞれツメ114および115が設けられ、ツメ114および115と対応する本体101の所定位置には、孔部116および117がそれぞれ設けられており、表示部102を本体101に閉塞した状態でツメ114および115がそれぞれ対応する孔部116および117に嵌合される。

【0106】これに対して表示部102は、本体101に閉塞された表示部102の前側が持ち上げられたときに、孔部116および117とツメ114および115の嵌合状態が解除され、表示部102が本体101から展開される。

【0107】また本体101は、その右側面にIrDA (Infrared Data Association) 準拠の赤外線ポート118、ヘッドフォン端子119、マイクロフォン用入力端子120、USB (Universal Serial Bus) 端子121、外部電源コネクタ122、外部ディスプレイ出力用コネクタ123、回転操作子の回転操作および押圧操作によって所定の処理を実行するための命令を入力するジョグダイヤル124およびモジュラジャック用のモデム端子125が設けられている。

【0108】また本体101は、その左側面に排気孔126、PCMCIA (Personal Computer Memory Card International Association) 規格のPC (Personal Computer) カードに対応したPCカードスロット127および4ピン対応のIEEE (Institute of Electrical and Electronics Engineers) 1394端子128が設けられている。

【0109】さらに本体101は、その後側面にバッテ

リコネクタ129が設けられており、底面にはバッテリーバック130を取り外すためのスライド式取り外しレバー131、およびスライド式取り外しレバー131のスライド操作をロックするロックレバー132が設けられるとともに、本体101の動作を中断して電源投入時の環境を再構築するためのリセットスイッチ133が設けられている。なお、バッテリーバック130は、バッテリーコネクタ129に対して着脱自在に接続される。

【0110】図10は、チケットレス端末3の内部の構成例を示す図である。

【0111】本体101の各種機能を統括的に制御するCPU150がホストバス152に接続されており、CPU150によってRAM153にロードされた各種プログラムやアプリケーションソフトウェアに応じた処理を、クロックジェネレータ160から与えられるシステムクロックに基づいて、所定の動作速度で実行することにより各種機能を実現するようになされている。またホストバス152には、キャッシュメモリ151が接続されており、CPU150が使用するデータをキャッシュし、高速アクセスを実現するようになされている。

【0112】このホストバス152は、PCI (Peripheral Component Interconnect) バス155とホスト-PCIブリッジ154を介して接続されており、PCIバス155にはビデオコントローラ156、IEEE1394インターフェース157、ビデオキャプチャ処理チップ183およびPCカードインターフェース158が接続されている。

【0113】ここでホスト-PCIブリッジ154は、CPU150と、ビデオコントローラ156、ビデオキャプチャ処理チップ183、IEEE1394インターフェース157およびPCカードインターフェース158との間で行われる各種データの授受を制御するとともに、メモリバス159を介して接続されたRAM153のメモリコントロールを行うようになされている。

【0114】またホスト-PCIブリッジ154は、ビデオコントローラ156とAGP (Accelerated Graphics Port) に沿った信号線を介して接続されており、これによりホスト-PCIブリッジ154およびビデオコントローラ156間で画像データを高速転送するようになされている。

【0115】ビデオキャプチャ処理チップ183は、シリアルバス182と接続されており、シリアルバス182を介してCCDカメラ107で撮像された画像データが供給されると、これを内蔵のフレームメモリ(図示せず)に一旦格納し、JPEG (Joint Photographic Experts Group) 規格に従って画像圧縮処理を施すことによりJPEG画像データを生成した後、そのJPEG画像データを再度フレームメモリに格納するようになされている。

【0116】ビデオキャプチャ処理チップ183は、CPU150からの要求に応じて、フレームメモリに格納されているJPEG画像データを、バスマスタ機能を用いてRA

M153へ転送した後、JPEG画像データとしてハードディスクドライブ（HDD）167へ転送する。

【0117】ビデオコントローラ156は、逐次供給される各種アプリケーションソフトウェアに基づく画像データや、CCDカメラ107で撮像された画像データを表示部102の液晶ディスプレイ109に出力することにより、複数のウィンドウ画面を表示するようになされている。

【0118】IEEE1394インターフェース157は、IEEE1394端子128と直結されており、IEEE1394端子128を介して他の装置やデジタルビデオカメラなどの外部デバイスと接続するようになされている。

【0119】PCカードインターフェース158は、オプション機能を追加するときに適宜PCカードスロット127に装着されるPCカード（図示せず）と接続され、PCカードを介して、ドライブと接続するようになされ、必要に応じて、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどが装着される。

【0120】PCIバス155は、ISA（Industrial Standard Architecture）バス165とPCI-ISAブリッジ166を介して接続されており、PCI-ISAブリッジ166にはHDD167およびUSB端子121が接続されている。

【0121】ここでPCI-ISAブリッジ166は、IDE（Intelligent Drive Electronics）インターフェース、コンフィギュレーションレジスタ、RTC（Real Time Clock）回路およびUSBインターフェース等によって構成されており、クロックジェネレータ160から与えられるシステムクロックを基にIDEインターフェースを介してHDD167を制御する。

【0122】HDD167のハードディスクには、Windows（登録商標）98などのOS（Operating System）、電子メールプログラム、オートパイロットプログラム、ジョグダイヤルサーバプログラム、ジョグダイヤルドライバ、キャプチャソフトウェア、およびこれら以外の各種アプリケーションソフトウェアが格納されており、起動処理の過程で逐次RAM153に転送されてロードされる。

【0123】PCI-ISAブリッジ166は、USB端子121を介して接続される図示せぬフレキシブルディスクドライブ、プリンタおよびUSBマウス等の外部デバイスを、USBインターフェースを介して制御するとともに、ISAバス165に接続されるモデム169およびサウンドコントローラ170を制御する。

【0124】モデム169は、モデム端子125から公衆回線網5を介してインターネットサービスプロバイダ6に接続し、さらにインターネットサービスプロバイダ6を介してインターネット7へダイヤルアップIP（Internet Protocol）接続するようになされている。

【0125】サウンドコントローラ170は、マイクロフォン113で集音された音声信号をデジタル変換する

ことにより音声データを生成し、これをCPU150に出力するとともに、CPU150から供給される音声データをアナログ変換することにより音声信号を生成し、これを内蔵スピーカ105を介して外部に出力する。

【0126】またISAバス165には、I/O（In/Out）コントローラ173が接続されており、外部電源コネクタ122から電源供給充電制御回路185を介して外部電源の電力供給を受け、電源スイッチ106がオンされたときに各回路へ電力の供給を行う。なお、ここでもI/Oコントローラ173は、クロックジェネレータ160から供給されるシステムクロックを基に動作する。

【0127】また電源供給充電制御回路185は、I/Oコントローラ173によって制御され、バッテリーコネクタ129に接続されたバッテリーパック130の充電を制御する。

【0128】I/Oコントローラ173は、マイクロコントローラ、I/Oインターフェース、CPU、ROM、RAM等によって構成されており、フラッシュメモリ179に格納されているBIOS（Basic Input/Output System）に基づいてOSやアプリケーションソフトウェアと液晶ディスプレイ109やHDD167等の各種周辺機器との間におけるデータの入出力を制御する。また、I/Oコントローラ173は、赤外線ポート118と接続され、例えば他の装置との間で赤外線通信を実行するようになされている。

【0129】さらにI/Oコントローラ173は、反転スイッチ177と接続されており、撮像部111が液晶ディスプレイ109の背面側方向に180度回転されたとき、反転スイッチ177がオンされ、その旨をPCI-ISAブリッジ166およびホスト-PCIブリッジ154を介してCPU150に通知する。

【0130】これに加えてI/Oコントローラ173は、全押し／半押しスイッチ178と接続されており、本体101の上面に設けられたシャッターボタン108が半押し状態にされたとき、全押し／半押しスイッチ178が半押し状態にオンされ、その旨をCPU150に通知するとともに、シャッターボタン108が全押し状態にされたとき、全押し／半押しスイッチ178が全押し状態にオンされ、その旨をCPU150に通知する。すなわち、CPU150は、HDD167のハードディスクからキャプチャソフトウェアをRAM153に立ち上げた状態で、ユーザによってシャッターボタン108が半押し状態にされると静止画像モードに入り、CCDカメラ107を制御して静止画像のフリーズを実行し、全押し状態にされるとフリーズされた静止画像データを取り込み、ビデオコントローラ156に出力する。

【0131】これに対してCPU150は、キャプチャソフトウェアを立ち上げない状態で、ユーザによってシャッターボタン108が全押し状態にされると動画像モードに入り、最大60秒程度の動画像を取り込み、ビデオコントローラ156に出力する。

【0132】ところで、I/Oコントローラ173のROMには、ウェイクアッププログラム、キー入力監視プログラム、LED制御プログラム、およびジョグダイヤル状態監視プログラム、その他種々の制御プログラムが格納されている。

【0133】ジョグダイヤル状態監視プログラムは、HDD167のハードディスクに格納されているジョグダイヤルサーバプログラムと連動して用いられるプログラムであり、ジョグダイヤル124が回転操作または押圧操作されたか否かを監視するためのプログラムである。

【0134】ウェイクアッププログラムは、PCI-ISAブリッジ166内のRTC回路から供給される現在時刻が予め設定した開始時刻と一致すると、CPU150によって所定の処理を実行するように制御されたプログラムであり、キー入力監視プログラムは、操作キー103およびその他の各種キースイッチからの入力を監視するプログラムである。LED制御プログラムは、電源ランプPL、電池ランプBL、メッセージランプML等の各種ランプの点灯を制御するプログラムである。

【0135】またI/Oコントローラ173のRAMには、ジョグダイヤル状態監視プログラム用のI/Oレジスタ、ウェイクアッププログラム用の設定時刻レジスタ、キー入力監視プログラム用のキー入力レジスタ、LED制御プログラム用のLED制御レジスタおよびその他の各種プログラム用のレジスタが設けられている。

【0136】設定時刻レジスタは、ウェイクアッププログラムで用いるためにユーザが予め任意に設定した開始時刻の時間情報を格納するようになされている。従って、I/Oコントローラ173は、ウェイクアッププログラムに基づいてRTC回路から供給される現在時刻が任意に設定した開始時刻と一致するか否かを判定し、開始時刻と一致したときには、その旨をCPU150に通知する。これにより、CPU150は、開始時刻で予め設定された所定のアプリケーションソフトウェアを立ち上げ、そのアプリケーションソフトウェアに従って、所定の処理を実行する。

【0137】またキー入力監視レジスタは、操作キー103、スティック104、左クリックボタン104A、右クリックボタン104B、およびセンタボタン105C等の入力操作に応じた操作キーフラグを格納するようになされている。

【0138】従ってI/Oコントローラ173は、キー入力監視プログラムに基づいて、例えば、スティック104によるポインティング操作や、左クリックボタン104A、右クリックボタン104B、およびセンタボタン104Cのクリック操作が行われたか否かを操作キーフラグの状態に基づいて判定し、ポインティング操作やクリック操作が行われたときには、その旨をCPU150に通知する。

【0139】ここでポインティング操作とは、スティッ

ク104を指で上下左右に押圧操作することによりマウスカーソルを画面上の所望位置に移動する操作のことであり、クリック操作とは左クリックボタン104Aまたは右クリックボタン104Bを指で素早く押して離す操作のことである。

【0140】これによりCPU150は、ポインティング操作によるマウスカーソルの移動やクリック操作に応じた所定の処理を実行する。

【0141】またLED制御レジスタは、電源ランプPL、電池ランプBL、メッセージランプML等の各種ランプの点灯状態を示す点灯フラグを格納するようになされている。

【0142】従ってI/Oコントローラ173は、例えば、ジョグダイヤル124の押圧操作によりCPU150がHDD167のハードディスクから電子メールプログラムを立ち上げ、その電子メールプログラムに従って電子メールを受け取ったときに点灯フラグを格納するとともに、その点灯フラグに基づいてLED181を制御することによりメッセージランプMLを点灯させる。

【0143】またジョグダイヤル状態監視プログラム用のI/Oレジスタは、ジョグダイヤル124に対する回転操作および押圧操作に応じた回転操作フラグおよび押圧操作フラグを格納するようになされている。

【0144】従ってI/Oコントローラ173は、回転検出部188を介して接続されたジョグダイヤル124の回転操作および押圧操作により複数のメニュー項目の中からユーザが所望するメニュー項目が選択されたとき、I/Oレジスタに格納されている回転操作フラグおよび押圧操作フラグを立てるとともに、その旨をCPU150に通知する。

【0145】これによりCPU150は、HDD167から読み出してRAM153上に立ち上げたジョグダイヤルサーバプログラムに従って、ジョグダイヤル124の回転操作および押圧操作によって決定されたメニュー項目に対応するアプリケーションソフトウェアを立ち上げて所定の処理を実行する。

【0146】ここでI/Oコントローラ173は、電源スイッチ106がオフでOSが起動していない状態であっても、電源供給充電制御回路185の制御によって常時動作しており、専用キーを設けることなく省電力状態または電源オフ時のジョグダイヤル124の押圧操作によってユーザが所望するアプリケーションソフトウェアやスクリプトファイルを起動するようになされている。

【0147】なお、I/Oコントローラ173は、シリアルバス182とも接続されており、操作キー103やジョグダイヤル124によって設定されたCCDカメラ107に対する各種設定パラメータをシリアルバス182を介して供給することにより、CCDカメラ107における明るさやコントラストを調整するようになされている。

【0148】図11は、チケットレス端末3の機能を説

10

20

30

40

50

明するブロック図である。

【0149】入出力管理プログラム191は、操作キー103、スティック式ポインティングデバイス104、もしくはジョグダイヤル124を用いて、ユーザが入力した操作または命令を示す信号を、対応するアプリケーションに供給したり、各種アプリケーションの処理に基づいて、所定のデータをIEEE1394端子128もしくはUSB端子121に出力して他の機器に送信させたり、CCDカメラ107で撮像された画像データを液晶ディスプレイ109に出力して画像を表示させる処理を管理するプログラムである。

【0150】サイバーコードファインダ(CyberCode Finder)(商標)192は、入出力管理プログラム191の処理によりユーザの操作に対応する信号、または他の機器から送信されてきた指令(コマンド)に対応する信号の供給を受け、その信号を基に、液晶ディスプレイ109に、所定の画面を表示させ、CCDカメラ107により画像を撮像する処理を実行するとともに、撮像された画像からサイバーコードのコード番号を認識する処理を実行するためのプログラムである。

【0151】認証プログラム193は、サイバーコードファインダ192の処理により認識されたサイバーコードのコード番号を基に、IEEE1394端子128もしくはUSB端子121を介して、サイバーコード認証サイト8にアクセスし、ユーザ認証の実行を要求し、サイバーコード認証サイト8から供給された認証結果を、液晶ディスプレイ109に表示させるためのプログラムである。

【0152】図12は、サイバーコード生成プログラム発行/認証サーバ11の電氣的内部の構成例を示す図である。

【0153】CPU201は、ROM202またはハードディスク装置204に記憶されているプログラムに従って、各種処理を実行するようになされている。ROM202は、例えば、起動時に実行されるプログラムや各種のデータを記憶している。RAM203は、CPU201により各種の処理が実行されるとき必要なデータやプログラムを記憶する。ハードディスク装置204は、このサイバーコード生成プログラム発行/認証サーバ11をサーバ*
SeedID=f (UID, TID)

【0160】上記式(1)において、UIDは、例えば、携帯電話機1のユーザ毎に割り当てられる固有のユーザIDを表わし、TIDは、サイバーコード生成プログラムの発行要求を受信した時刻(すなわち、サイバーコード生成プログラム発行開始時刻)を表わす。作成された乱数発生用SeedIDは、後述するように、サイバーコード生成プログラムを作成するときに利用される。

【0161】ここで乱数(random numbers)について説明する。乱数とは、一般に数の集合から、無作為抽出で抜き出された数を示すものであり、真性乱数、物理乱数、および擬似乱数(pseudo random number)がある。

*して機能させるサーバプログラムや、図13を用いて後述する各種のプログラムを記憶している。

【0154】表示部205は、LCDもしくはCRT(Cathode Ray Tube)などからなり、CPU201より供給される画像データに対応する画像を表示するようになされている。入力部206は、キーボード、ボタン、スイッチもしくはマウスなどからなり、CPU201に各種の指令を入力するとき、サイバーコード生成プログラム発行/認証サーバ11の管理者により操作される。

10 【0155】ネットワークインターフェース207は、インターネット7に接続され、サイバーコード生成プログラム発行/認証サーバ11宛のIPパケットを受信するとともに、CPU201より供給されたデータから、インターネット7のネットワークに従ってIPパケットを生成し、インターネット7に出力する。

20 【0156】ドライブ208には、必要に応じて、磁気ディスク211、光ディスク212、光磁気ディスク213、または半導体メモリ214などが装着され、CPU201が実行するプログラムなどがインストールされる。

【0157】図13は、サイバーコード生成プログラム発行/認証サーバ11の機能を説明するブロック図である。

30 【0158】入出力管理プログラム221は、入力部206を用いて、ユーザが入力した操作または命令を示す信号もしくはネットワークインターフェース207から入力される信号を、対応するアプリケーションに供給したり、各種アプリケーションの処理に基づいて、所定のデータをネットワークインターフェース207に出力して他の機器に送信させたり、所定の画像データを表示部205に出力して画像を表示させる処理を管理するプログラムである。

【0159】Seed作成プログラム222は、入出力管理プログラム221の処理により他の機器から送信されてきた指令(サイバーコード生成プログラムの発行要求)に対応する信号の供給を受け、その信号を基に、ユーザIDを生成(発行)し、さらに次式(1)に従って、乱数発生用SeedIDを作成する。

$$\dots (1)$$

40 【0162】真性乱数は、ビット列にすると、0と1の発生確率がそれぞれ1/2で、各ビットは他の部分と独立なiid(independent and identically distributed)である。

【0163】物理乱数は、量子力学の効果を増幅してデジタル化したものであり、平滑化して0および1のバランスをとれば、真性乱数になるものである。

50 【0164】疑似乱数は、種(seed)と呼ばれる入力ビットパターンを基に計算された、種よりも長いランダムに見えるビット・パターンであり、歪と周期がある。なお、疑似乱数は、決定的(deterministic)アルゴリズムから

生成されるので、種が決まれば出力乱数は一意に決まるため、暗号に使う時には、種を秘密にする必要がある。Seed作成プログラム 222 は、この擬似乱数を使用する。すなわち、作成されるサイバーコード生成プログラムには、この擬似乱数が使用され、基となる種はSeed作成プログラム 222 により生成される。

【0165】図 13 の説明に戻る。サイバーコード生成プログラム発行部 223 は、入出力管理プログラム 221 の処理により他の機器から送信されてきた指令（サイバーコード生成プログラムの発行要求）に対応する信号の供給を受けてSeed作成プログラム 222 の処理により作成された乱数発生用SeedID、発行要求のあった携帯電話機 1 のユーザを表わすユーザID (UID)、および、サイバーコード生成プログラム発行開始時刻TIDを基に、例えば、

P(UID, TID, SeedID) (t)

で表わされるようなユーザ毎に固有のサイバーコード生成プログラムPID (Java (登録商標) アプレット) を作成する。

【0166】サイバーコード生成プログラム発行/認証サーバ 11 は、このユーザ毎に固有のアルゴリズムを持ったプログラムを、ユーザに配布することにより、アルゴリズム自体を認証キーとして利用することができる。

【0167】サイバーコード生成プログラム発行部 223 は、作成されたユーザ毎に固有のサイバーコード生成プログラムPIDを、インターネット 7、インターネットサービスプロバイダ 6、公衆回線網 5、基地局 2 を介して、発行要求のあった携帯電話機 1 に送信する。

【0168】認証用キー分離プログラム 224 は、入出力管理プログラム 221 の処理により他の機器から送信されてきた指令（サイバーコード生成プログラムの実行により生成されたサイバーコードのコード番号）に対応する信号の供給を受け、コード番号に含まれるユーザIDを分離する。例えば、8桁で表わされるコード番号のうち、下4桁がユーザIDとして埋め込まれている場合、上4桁と下4桁のコード番号に分離される。

【0169】認証プログラム 225 は、入出力管理プログラム 221 の処理によりチケットレス端末 3 から送信されてきた指令（サイバーコード生成プログラムの実行により生成されたサイバーコードのコード番号）に対応する信号の供給を受けて認証用キー分離プログラム 224 の処理により分離されたユーザIDを基に、登録ユーザ情報データベース 12 から、対応するユーザIDの発行開始時刻TIDおよび乱数発生用SeedIDを検索する。

【0170】認証プログラム 225 は、ユーザID、検索された開始時刻TIDおよび乱数発生用Seedから、サイバーコード生成プログラムPIDを作成し、コード番号受信時刻を基にそのプログラムを実行する。認証プログラム 225 は、サイバーコード生成プログラムPIDの実行により生成されたサイバーコードのコードパターンから得

られるコード番号と、受信したコード番号とを比較し、一致すれば認証に成功した旨を、入出力管理プログラム 221、ネットワークインターフェース 207、およびインターネット 7 を介してチケットレス端末 3 に送信する。なお、認証に失敗した場合にも、その旨が同様に送信される。

【0171】次に、図 14 を参照して、本発明に係るサイバーコードについて説明する。

【0172】サイバーコードは、図 14 に示されるように、ロゴマーク部 231 とコード部 232 から構成されており、これらロゴマーク部 231 とコード部 232 の全体は、例えば、1 個の正方形のセルの矩形領域を 1 ブロックと表現すると、縦方向が 9.5 ブロックの長さで、横方向が 7 ブロック分の長さの長方形の領域内に配置されている。

【0173】ロゴマーク部 231 は、ロゴマーク、文字、または数字など、サイバーコードに関連する白抜き可読文字情報が表示されている。ここで、例えば、ロゴマークとしては、サイバーコードのコード体系に付された「CyberCode」など、何を意味するコードなのかを、人間が判読可能なマークとして、白抜き文字で表示される。

【0174】コード部 232 は、7×7 の全 49 個のブロック（またはセル）がマトリクス状に配置されたマトリクス構造を有し、1 つのサイバーコードで 24 ビットの情報をコード化し得るように構成されている。具体的には、四隅のブロック（コーナセル）およびその周囲の 3 ブロックを含む全 16 ブロック（16 ビット）はデータを構成せず、また残り 33 ブロック（33 ビット）中、9 ブロック（9 ビット）は、コードデータが正しいコードデータであることを確かめるためのチェックデータを構成する。従って、コード部 232 には、24 ビットのビットコードで表わされるサイバーコードの識別番号（コード番号）が設定される。

【0175】コード部 232 は、7×7 の全 49 個のブロックで構成させる以外に、8×8 の全 64 個のブロック（またはセル）で構成させるようにしてもよい。これにより、より多くの情報をコード化することが可能になる。

【0176】ID部 233 は、コード部 232 においてコード化された 24 ビットのデータを 16 進数で表わしたものであり、サイバーコードとして必須の部位ではない。

【0177】なお、サイバーコードの詳細については、特開 2000-82108 号および特開 2000-148904 号公報に開示されている。

【0178】次に、図 15 のフローチャートを参照して、携帯電話機 1 が、認証サイト 8 にアクセスし、コンサート会場 4 に入場するための入場チケットの代替となるサイバーコード（認証キー）を生成するためのサイバ

ーコード生成プログラムをダウンロードする処理について説明する。

【0179】ステップS1において、携帯電話機1の入出力制御プログラム81は、操作キー41もしくはジョグダイヤル44を用いてユーザが入力した操作を示す信号を表示プログラム83に供給し、例えば、図16に示されるようなメニュー画面を液晶ディスプレイ35に表示させる。

【0180】図16に示すメニュー画面には、ユーザが選択可能な、「メール」、「ダウンロード」、および「Java（登録商標）アプレット」などの項目が表示されている。ユーザが、操作キー41もしくはジョグダイヤル44を用いて、「ダウンロード」の項目を選択すると、入出力制御プログラム81は、ユーザが入力した操作を示す信号をウェブブラウザ82に供給する。

【0181】ウェブブラウザ82は、データ通信プログラム87に対して、アンテナ31、基地局2、公衆回線網5、インターネットサービスプロバイダ6、およびインターネット7を介して、サイバーコード認証サイト8のサイバーコード生成プログラム発行／認証サーバ11との通信を実行させる。

【0182】ステップS11において、サイバーコード認証サイト8のサイバーコード生成プログラム発行／認証サーバ11は、所定の通信処理を実行し、通信が確立した旨を、インターネット7、インターネットサービスプロバイダ6、公衆回線網5、および基地局2を介して、携帯電話機1に通知（送信）する。このとき、サーバのトップページに対応するコンパクトHTMLファイルも携帯電話機1に送信される。

【0183】ステップS2において、携帯電話機1のデータ通信プログラム87は、アンテナ31を介して、サイバーコード生成プログラム発行／認証サーバ11より、通信確立の通知を受け、さらに、受信したコンパクトHTMLファイルを表示プログラム83に供給し、例えば、図17に示されるようなダウンロード画面（トップページ）を液晶ディスプレイ35に表示させる。

【0184】図17に示すダウンロード画面には、ユーザが選択可能な、「認証用サイバーチケット」、および「認証用貨幣」などの項目が表示されている。ユーザが、操作キー41もしくはジョグダイヤル44を用いて、「認証用サイバーチケット」の項目を選択すると、入出力制御プログラム81は、ユーザが入力した操作を示す信号をウェブブラウザ82に供給する。

【0185】ウェブブラウザ82は、データ通信プログラム87に対して、アンテナ31、基地局2、公衆回線網5、インターネットサービスプロバイダ6、およびインターネット7を介して、サイバーコード認証サイト8のサイバーコード生成プログラム発行／認証サーバ11に、ユーザが入力した操作を示す信号を送信させ、サイバーコード生成プログラム発行／認証サーバ11から対

応するHTMLファイルを受信させ、表示プログラム83に供給させる。

【0186】表示プログラム83は、供給されたHTMLファイルを基に、例えば、図18に示されるようなサイバーチケットダウンロード画面を液晶ディスプレイ35に表示させる。

【0187】図18に示すサイバーチケットダウンロード画面には、ユーザが選択可能（ダウンロード可能）な、「△×試合」、「×○映画入場」、「○△コンサート」、「×□試合」、および「□○コンサート」の項目が表示されている。ユーザが、操作キー41もしくはジョグダイヤル44を用いて、「○△コンサート」の項目を選択すると、入出力制御プログラム81は、ユーザが入力した操作を示す信号をウェブブラウザ82に供給する。

【0188】ウェブブラウザ82は、表示プログラム83に対して、例えば、図19に示されるようなユーザ登録画面を液晶ディスプレイ35に表示させる。

【0189】図19に示すユーザ登録画面には、「○△コンサート認証用サイバーチケットをダウンロードするためのユーザIDを登録しますか？」といったメッセージとともに、その選択を促す「Yes」および「No」の項目を表示させる。ユーザが、操作キー41もしくはジョグダイヤル44を用いて、「Yes」の項目を選択すると、入出力制御プログラム81は、ユーザが入力した操作を示す信号をウェブブラウザ82に供給する。

【0190】ウェブブラウザ82は、データ通信プログラム87に対して、アンテナ31、基地局2、公衆回線網5、インターネットサービスプロバイダ6、およびインターネット7を介して、サイバーコード認証サイト8のサイバーコード生成プログラム発行／認証サーバ11に、ユーザが入力した操作を示す信号を送信させる。これにより、サイバーコード生成プログラム発行／認証サーバ11に対して、サイバーコード生成プログラムの発行が要求される。

【0191】ステップS12において、サイバーコード生成プログラム発行／認証サーバ11の入出力管理プログラム221は、携帯電話機1から、ネットワークインターフェース207を介してサイバーコード生成プログラムの発行要求を受けて、その要求を示す信号をSeed作成プログラム222に供給し、乱数発生用SeedIDを作成させる。

【0192】Seed作成プログラム222は、サイバーコード生成プログラムの発行要求を受信した現在時刻TIDを取得し、その時刻TIDを基に、ユーザ毎に固有のユーザIDを生成するとともに、生成されたユーザIDおよび時刻TIDを基に、上記式（1）に従って、乱数発生用SeedIDを作成する。

【0193】ステップS13において、サイバーコード生成プログラム発行部223は、ステップS12の処理

で作成された乱数発生用SeedID、ユーザID、および時刻TIDを基に、サイバーコード生成プログラムPIDを作成する。ここで作成されるサイバーコード生成プログラムPIDは、そのプログラムが実行されることにより生成されるサイバーコードのコード番号(ID部233)の下4桁に、ユーザIDが埋め込まれるようになされている。すなわち、認証時に、ユーザIDが必要とされるため、コード番号にユーザIDが埋め込まれるようになされている。

【0194】ステップS14において、サイバーコード生成プログラム発行部223は、サイバーコード生成プログラムPIDの作成に成功したか否かを判定し、サイバーコード生成プログラムPIDの作成に成功したと判定した場合、ステップS15に進み、生成されたユーザIDに対応付けて、サイバーコード生成プログラム発行開始時刻TIDおよび乱数発生用SeedIDを、登録ユーザ情報データベース12に記録させる。

【0195】ステップS16において、サイバーコード生成プログラム発行部223は、ステップS13の処理で作成されたサイバーコード生成プログラムPIDを、入出力管理プログラム221、ネットワークインターフェース207、インターネット7、インターネットサービスプロバイダ6、公衆回線網5、および基地局2を介して、携帯電話機1に送信する。

【0196】これに対して、ステップS14において、システムエラーなどによりサイバーコード生成プログラムPIDの作成に成功しなかった、すなわち、サイバーコード生成プログラムPIDの作成に失敗したと判定された場合、ステップS17に進み、サイバーコード生成プログラム発行部223は、サイバーコード生成プログラムの作成に失敗した旨を、入出力管理プログラム221、ネットワークインターフェース207、インターネット7、インターネットサービスプロバイダ6、公衆回線網5、および基地局2を介して、携帯電話機1に送信する。

【0197】ステップS3において、携帯電話機1のデータ通信プログラム87は、アンテナ31を介して、サイバーコード生成プログラム発行/認証サーバ11からサイバーコード生成プログラムの作成失敗の通知を受信したか否かを判定し、サイバーコード生成プログラムの作成失敗の通知を受信したと判定した場合、ステップS4に進み、受信したサイバーコード生成プログラムの作成失敗の通知を示す信号を表示プログラム83に供給する。表示プログラム83は、供給された信号に基づいて、例えば、「サイバーコード生成プログラムのダウンロードに失敗しました」といったエラーメッセージを液晶ディスプレイ35に表示させる。

【0198】ステップS3において、サイバーコード生成プログラムの作成失敗の通知を受信していないと判定された場合、ステップS5に進み、携帯電話機1のデータ通信プログラム87は、アンテナ31を介して、サイ

バーコード生成プログラム発行/認証サーバ11から送信されてきたサイバーコード生成プログラムPIDを受信し、それをJava(登録商標)アプレット91としてメモリ86に記録させる。

【0199】ステップS4もしくはステップS5の処理の後、ステップS6において、ウェブブラウザ82は、データ通信プログラム87に対して、サイバーコード生成プログラム発行/認証サーバ11との通信を解除させ、処理は終了される。

10 【0200】以上の処理により、携帯電話機1は、ユーザ毎に固有のサイバーコード生成プログラムPIDを取得することができ、図20を用いて後述する、サイバーコード生成プログラムの実行により生成されるサイバーコードを認証キーとして利用することができる。

【0201】次に、図20のフローチャートを参照して、携帯電話機1のユーザが、上述した処理によって取得(ダウンロード)したサイバーコード生成プログラムPIDを実行して、コンサート会場4で開催されるコンサートの入場チケットの代替となるサイバーコードを生成し、そのサイバーコードをチケットレス端末3で認識させ、認識されたコード番号を、サイバーコード認証サイト8で認証させる処理について説明する。

【0202】携帯電話機1のユーザは、操作キー41もしくはジョグダイヤル44を用いて、図16に示したようなメニュー画面を液晶ディスプレイ35に表示させ、「Java(登録商標)アプレット」の項目を選択する。これにより、ステップS31において、Java(登録商標)アプレット実行プログラム85は、ユーザが入力した操作を示す信号を表示プログラム83に供給し、図21に示されるようなJava(登録商標)アプレット実行画面を液晶ディスプレイ35に表示させる。

30 【0203】図21に示すJava(登録商標)アプレット実行画面には、ユーザによってダウンロードされた、「○△コンサート」、および「×○映画入場」などのJava(登録商標)アプレット(サイバーコード生成プログラムPID)の項目が表示されている。ユーザが、操作キー41もしくはジョグダイヤル44を用いて、「○△コンサート」の項目を選択すると、Java(登録商標)アプレット実行プログラム85は、選択された「○△コンサート」に対応するサイバーコード生成プログラムPIDを実行する。

【0204】ステップS32において、Java(登録商標)アプレット実行プログラム85は、現在時刻Tuを基に、サイバーコードを生成し、生成されたサイバーコードを液晶ディスプレイ35に表示させる。これにより、例えば、図22に示されるように、「○△コンサート認証用サイバーチケット」といったサイバーコードの内容を示す情報および現在時刻とともに、生成されたサイバーコード(認証用サイバーチケット)241が表示される。

【0205】ところで、サイバーコード生成プログラムPIDが実行されると、現在時刻を基にサイバーコード241が生成されるが、このサイバーコード241は、図23に示されるように、所定の時間（例えば、10秒）毎に更新（変化）される。

【0206】図23の例の場合、時刻 t_1 を基にサイバーコード241-1が生成され、時刻 t_2 を基にサイバーコード241-2が生成され、時刻 t_3 を基にサイバーコード241-3が生成され、時刻 t_4 を基にサイバーコード241-4が生成され、同様に、所定の時間毎にサイバーコード241が生成される。

【0207】すなわち、携帯電話機1でサイバーコードが生成されてから、そのコードパターンがチケットレス端末3で認識されることにより得られるコード番号がサイバーコード認証サイト8に送信され、サイバーコード認証サイト8でコード番号に含まれるユーザIDが分離され、分離されたユーザIDを基に、乱数発生用SeedIDが作成され、作成された乱数発生用SeedID、ユーザID、およびコード番号受信時刻からサイバーコード生成プログラムPIDが再度作成され、そのプログラムを実行することによって生成されるサイバーコードは、携帯電話機1で作成されたサイバーコードと同一時刻に作成されたものであるとして保証するようになされている。

【0208】図23の例においては、時刻 t_3 を基にサイバーコード241-2が生成され、時刻 t_a でサイバーコード241-2が認識され、認識されたコードパターンから得られるコード番号がサイバーコード認証サイト8に送信され、サイバーコード認証サイト8において、時刻 t_b を基に生成されるサイバーコード242とは同一のものであるとすることができる。

【0209】このように、携帯電話機1でサイバーコード生成プログラムPIDが実行される時刻 t_u と、サイバーコード認証サイト8で再度サイバーコード生成プログラムPIDが作成され、そのプログラムが実行される時刻 t_s は、同一時刻であるものとすることができる。すなわち、所定の時間内に同一のサイバーコード生成プログラムPIDが実行され、サイバーコードが生成されたとして認証される。なお、サイバーコード241が生成される時間間隔を短くすることによって、生成されたサイバーコードの有効期限が短くなり、コードの盗用による認証性が減少するため、認証精度を向上させることができる。

【0210】図20の説明に戻る。ステップS33において、携帯電話機1のユーザは、液晶ディスプレイ35に表示されているサイバーコード241を、チケットレス端末3のCCDカメラ107にかざし、サイバーコード241が撮像されるようにその位置を調整する。

【0211】このとき、チケットレス端末3では、予めサイバーコードファインダ192が起動されており、液晶ディスプレイ109に、例えば、図24に示されるよ

うな画面が表示されている。

【0212】ステップS41において、チケットレス端末3のサイバーコードファインダ192は、CCD107により画像を撮像する処理を実行させるとともに、撮像された画像からサイバーコードを認識する処理を実行する。このとき、液晶ディスプレイ109に表示されている画面は、例えば、図25に示されるように、「認証中」といったメッセージを表示させ、ユーザに対して、サイバーコードの認証中である旨を知らしめる。

【0213】サイバーコードファインダ192は、撮像された画像からサイバーコードのコードパターンから得られるコード番号を認識する。ステップS42において、認証プログラム193は、認識されたコード番号をサイバーコード認証サイト8に送信し、ユーザ認証の実行を要求する。

【0214】ステップS51において、サイバーコード認証サイト8のサイバーコード生成プログラム発行／認証サーバ11は、チケットレス端末3から送信されてきたコード番号を受信し、ユーザ認証の要求を受ける。ステップS52において、サイバーコード生成プログラム発行／認証サーバ11の認証用キー分離プログラム224は、ステップS51の処理で受信されたコード番号から、ユーザIDを分離する。

【0215】ステップS53において、認証プログラム225は、ステップS52の処理で分離されたユーザIDを基に、登録ユーザ情報データベース12から、対応するユーザIDの発行開始時刻TIDおよび乱数発生用SeedIDを検索する。ステップS54において、認証プログラム225は、ステップS52の処理で分離されたユーザID、ステップS53の処理で検索された時刻TIDおよび乱数発生用SeedIDから、サイバーコード生成プログラムPIDを再度作成する。

【0216】ステップS55において、認証プログラム225は、コード番号受信時刻を基に、ステップS54の処理で作成されたサイバーコード生成プログラムPIDを実行し、サイバーコード242を生成する。ステップS56において、認証プログラム225は、ステップS55の処理により生成されたサイバーコード242のコードパターンから得られるコード番号と、ステップS51の処理で受信したコード番号から、一方向性マッチング（認証処理）を行う。

【0217】認証処理としては、サイバーコードのコード番号の有効期限が切れていないか（例えば、以前に開催されたコンサートの認証用サイバーチケットがコピーされたものであり、コンサート開催日を過ぎていないか）、もしくは、認証されたサイバーコードが、所定のユーザID、時刻TID、および乱数発生用SeedIDから作成されたものではないか（例えば、別のサイバーコード生成プログラムPIDにより作成されたものであるか）などを判定する。

【0 2 1 8】ステップ S 5 7 において、認証プログラム 2 2 5 は、認証結果を、入出力管理プログラム 2 2 1、ネットワークインターフェース 2 0 7、およびインターネット 7 を介してチケットレス端末 3 に送信する。

【0 2 1 9】ステップ S 4 3 において、チケットレス端末 3 の認証プログラム 1 9 3 は、サイバーコード認証サイト 8 から供給された認証結果を、液晶ディスプレイ 1 0 9 に表示させる。これにより、例えば、図 2 6 に示されるように、「認証に成功しました!」といったメッセージが表示される。

【0 2 2 0】以上のように、サイバーコード認証サイト 8 は、サイバーコード発行要求のあった携帯電話機 1 のユーザのユーザ ID、サイバーコード生成プログラム発行要求を受信した時刻 TID、および乱数発生用 SeedID から、サイバーコード生成プログラム PID を作成し、作成されたプログラムを要求元のユーザに配布するとともに、それらの情報を登録ユーザ情報データベース 1 2 に記録しておく。そして、サイバーコード認証サイト 8 は、認証時に、チケットレス端末 3 から送信されてくるコード番号に含まれるユーザ ID を基に、登録情報データベース 1 2 から対応する時刻 TID および乱数発生用 SeedID を取得して、再びサイバーコード生成プログラム PID を作成し（すなわち、認証しようとするユーザと同一のサイバーコード生成プログラム PID を作成し）、サイバーコードを生成し、それを認証するようにしたので、サイバーコード生成プログラム自体に認証キーの機能を持たせることができる。

【0 2 2 1】また、時刻を基にサイバーコードが生成されるため、認証時において唯一のサイバーコードであるという有効期限付きの認証キーとして利用することが可能になる。

【0 2 2 2】また、サイバーコードのコード番号の下 4 桁に、ユーザ ID を埋め込むようにして説明したが、本発明はこれに限られるものではなく、例えば、図 2 7

(A) に示されるように、サイバーコード 2 4 1 のビットパターンの一部（例えば、ブロック 2 5 1 - 1 および 2 5 1 - 2）がユーザ ID として埋め込まれるか、図 2 7 (B) に示されるように、複数毎のサイバーコード 2 4 1 - 1 乃至 2 4 1 - 4 が時系列的に配置され、それらのコードで 1 つのコード番号が表わされるようにして、その 1 枚（例えば、サイバーコード 2 4 1 - 3）がユーザ ID として埋め込まれるか、もしくは、図 2 7 (C) に示されるように、複数毎のサイバーコード 2 4 1 - 1 乃至 2 4 1 - 4 が空間的に配置され、それらのコードで 1 つのコード番号が表わされるようにして、その 1 枚（例えば、サイバーコード 2 4 1 - 2）がユーザ ID として埋め込まれるようにしてもよい。

【0 2 2 3】また、以上説明したチケットレスシステムにおいては、i - アプリの制約に基づく問題点を解消することも可能である。すなわち、i - アプリにおいて

は、一般的に以下のような制約があることが知られている。

(1) i アプリでは、セキュリティ保護のため、プログラム内部の処理を用いて、そのプログラムのダウンロード元のサイトにしか、アクセスすることができない。

(2) また、セキュリティ保護のため、プログラム内部の処理により、任意の場所（サイト）に電話をかけて通信を確立することは許可されていない。

10 【0 2 2 4】従って、Java（登録商標）アプレットを用いて携帯電話機が認証のために、所定の認証サーバに通信するとなると、Java（登録商標）アプレット発行サーバと認証サーバが同一である必要がある。

【0 2 2 5】また、ユーザ毎に唯一の認証プログラムを有するようにするためには、全てのイベントを一括して行うような認証サーバを構成する必要がある。

20 【0 2 2 6】これに対して、本発明のチケットレスシステムによれば、サイバーコード生成プログラム（Java（登録商標）アプレット）がダウンロードされた携帯電話機 1 がサイバーコード生成プログラム発行／認証サーバ 1 1 に通信するのではなく、チケットレス端末 3 がサイバーコード生成プログラム発行／認証サーバ 1 1 に通信するため、アクセス先の制限を受けることがなくなる。

【0 2 2 7】また、イベント毎にサイバーコード生成プログラム発行／認証サーバ 1 1 を設けることが可能となり、ユーザは、ユーザ毎に唯一のサイバーコード生成プログラムをダウンロードすることができるとともに、イベント毎に異なる認証サーバにアクセスすることができ

30 【0 2 2 8】また、チケットレス端末 3 で携帯電話機 1 の液晶ディスプレイ 3 5 に表示されたサイバーコード 2 4 1 が認識され、インターネット 7 などのネットワークを介してサイバーコード認証サイト 8 のサイバーコード生成プログラム発行／認証サーバ 1 1 でユーザ認証を行うものとして説明したが、本発明はこれに限られるものではなく、チケットレス端末 3 とサイバーコード生成プログラム発行／認証サーバ 1 1 を 1 つの装置として構成することも可能である。

40 【0 2 2 9】さらに、携帯電話機 1 にサイバーコード生成プログラムをダウンロードし、そのプログラムを実行してサイバーコードを表示させるものとして説明したが、本発明はこれに限られるものではなく、例えば、表示機能を有し、かつ、サイバーコード生成プログラム（Java（登録商標）アプレット）が実行可能な携帯型パーソナルコンピュータ、ポータブルデバイス、PDA（Personal Digital Assistant）、もしくは PHS（Personal Handyphone System）などの装置全般に広く適用することができる。

50 【0 2 3 0】また、以上においては、サイバーコード生成プログラム自体が認証キーとしての機能を持っている

ため、そのプログラムの実行により生成されるものは、サイバーコードの他、数字の配列、音声、もしくは絵柄などでもよい。

【0 2 3 1】また、以上においては、携帯電話機 1 の液晶ディスプレイ 3 5 に表示されるサイバーコードを認証用サイバーチケットとして利用するものとしたが、例えば、図 1 7 に示したダウンロード画面において、ユーザによって、「認証用貨幣」の項目が選択された場合、ユーザが取引している所定の銀行にアクセスされ、ユーザの口座から所定金額の代替になる認証用貨幣コインを生成するためのサイバーコード生成プログラムがダウンロードされるようにしてもよい。この場合、ユーザが、所望の物品を購入する際に、サイバコード認識可能な自動販売機や店頭端末において、ユーザが携帯電話機 1 の液晶ディスプレイ 3 5 に認証用貨幣（サイバーコード）を表示させ、上述したようにして認証されると、電子決済が実行される。

【0 2 3 2】さらにまた、以上においては、様々なサイバーコード生成プログラム（Java（登録商標）アプレット）が携帯電話機 1 にダウンロードされることにより、メモリ 8 6 の記憶容量が一杯になってしまうため、例えば、有効期限を過ぎた（既にコンサートが終了している）認証用サイバーチケットを自動消滅させるようにしたり、もしくは、図 2 1 に示した Java（登録商標）アプレット実行画面において、ユーザによって、有効期限を過ぎた Java（登録商標）アプレットが選択された場合、「有効期限が過ぎているため、プログラムを実行することができません」といった警告メッセージを液晶ディスプレイ 3 5 に表示させるようにしてもよい。

【0 2 3 3】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを記録する記録媒体は、図 1 2 に示すように、磁気ディスク 2 1 1（フレキシブルディスクを含む）、光ディスク 2 1 2（CD-ROM (Compact Disc-Read Only Memory)、DVD (Digital Versatile Disc)を含む）、光磁気ディスク 2 1 3（MD (Mini-Disc)（登録商標）を含む）、もしくは半導体メモリ 2 1 4 などよりなるパッケージメディア、または、プログラムが一時的もしくは永続的に格納される Flash ROM や、ハードディスクなどにより構成される。記録媒体へのプログラムの記録は、必要に応じてルータ、モデムなどのインターフェースを介して、公衆回線網 5、ローカルエリアネットワークまたはインターネット 7、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0 2 3 4】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理も含むものである。

【0 2 3 5】また、本明細書において、システムとは、

複数の装置により構成される装置全体を表すものである。

【0 2 3 6】

【発明の効果】本発明の情報提供装置および方法、並びに第 1 のプログラムによれば、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザ ID を発行し、発行されたユーザ ID、および発行要求の受信時刻を基に、乱数を発生し、発生された乱数、ユーザ ID、および受信時刻を基に、所定画像を生成するためのプログラムを作成し、作成されたプログラムを情報処理装置に提供するようにしたので、プログラムを認証キーとして機能させることができる。

【0 2 3 7】また本発明の情報処理装置および方法、並びに第 2 のプログラムによれば、情報提供装置に対してプログラムの送信を要求し、情報提供装置から提供されるプログラムを受信し、受信されたプログラムを実行して所定画像を生成し、生成された所定画像を表示するようにしたので、ユーザは、表示された画像を認証キーとして利用することができる。

【0 2 3 8】また本発明の情報認証装置および方法、並びに第 3 のプログラムにおいては、第 1 の画像を撮像し、撮像された第 1 の画像に対応する第 1 の情報を認識し、認識された第 1 の情報に含まれるユーザ ID を基に、他の装置に記録されているユーザ情報を検索し、検索されたユーザ情報を基に、第 2 の画像を生成するためのプログラムを作成し、作成されたプログラムを実行して第 2 の画像を生成し、生成された第 2 の画像に対応する第 2 の情報と、認識された第 1 の情報を認証するようにしたので、高精度にユーザ認証することができる。

【0 2 3 9】さらにまた本発明の認証システムによれば、情報提供装置が、情報処理装置から送信されてくるプログラムの発行要求を受けて、情報処理装置に対して、ユーザ ID を発行し、発行されたユーザ ID、および発行要求の受信時刻を基に、乱数を発生し、発生された乱数、ユーザ ID、および受信時刻を基に、第 1 の画像を生成するための第 1 のプログラムを作成し、作成された第 1 のプログラムを情報処理装置に提供し、ユーザ ID に対応付けて、乱数および受信時刻を記録し、情報処理装置が、情報提供装置に対して第 1 のプログラムの送信を要求し、情報提供装置から提供される第 1 のプログラムを受信し、受信された第 1 のプログラムを実行して第 1 の画像を生成し、生成された第 1 の画像を表示し、情報認証装置で、情報処理装置に表示されている第 1 の画像を撮像し、撮像された第 1 の画像に対応する第 1 の情報を認識し、認識された第 1 の情報に含まれるユーザ ID を基に、情報提供装置に記録されている乱数および受信時刻を検索し、検索された乱数および受信時刻を基に、第 2 の画像を生成するための第 2 のプログラムを作成し、作成された第 2 のプログラムを実行して第 2 の画像を生成し、生成された第 2 の画像に対応する第 2 の情報と、

10

20

30

40

50

認識された第1の情報を認証するようにしたので、プログラム自体をユーザ毎に変化させて、それを認証キーとして機能させることにより、高精度にユーザ認証することができる。

【図面の簡単な説明】

【図1】本発明を適用したチケットレスシステムの一実施の形態の構成例を示す図である。

【図2】登録ユーザ情報データベースに記録されているユーザ情報の記録例を示す図である。

【図3】携帯電話機の外観の構成例を示す図である。

【図4】携帯電話機の表示部の外観の構成例を示す図である。

【図5】携帯電話機の内部の構成例を示すブロック図である。

【図6】携帯電話機の機能を説明するブロック図である。

【図7】チケットレス端末の外観の構成例を示す斜視図である。

【図8】図7のチケットレス端末の表示部を閉じた状態の構成を示す左側面図である。

【図9】図7のチケットレス端末の表示部を閉じた状態の構成を示す背面図である。

【図10】チケットレス端末の内部の構成例を示す図である。

【図11】チケットレス端末の機能を説明するブロック図である。

【図12】サイバーコード生成プログラム発行／認証サーバの内部の構成例を示す図である。

【図13】サイバーコード生成プログラム発行／認証サーバの機能を説明するブロック図である。

【図14】サイバーコードを説明する図である。

【図15】サイバーコード生成プログラムのダウンロード処理を説明するフローチャートである。

【図16】携帯電話機の液晶ディスプレイに表示されるメニュー画面を示す図である。

【図17】携帯電話機の液晶ディスプレイに表示される

ダウンロード画面を示す図である。

【図18】携帯電話機の液晶ディスプレイに表示されるサイバーチケットダウンロード画面を示す図である。

【図19】携帯電話機の液晶ディスプレイに表示されるユーザ登録画面を示す図である。

【図20】サイバーコードの認証処理を説明するフローチャートである。

【図21】携帯電話機の液晶ディスプレイに表示されるJava（登録商標）アプレット実行画面を示す図である。

【図22】携帯電話機の液晶ディスプレイに表示されるサイバーコードを示す図である。

【図23】生成されるサイバーコードが変化する様子を説明する図である。

【図24】サイバーコードファインダ起動時に表示される画面を示す図である。

【図25】サイバーコード認証中に表示される画面を示す図である。

【図26】サイバーコードが認識された場合に表示される画面を示す図である。

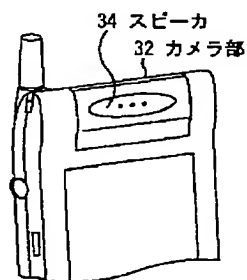
【図27】ユーザIDの埋め込み方法を説明する図である。

【符号の説明】

1 カメラ付デジタル携帯電話機, 3 チケットレス端末, 7 インターネット, 8 サイバーコード認証サイト, 11 サイバーコード生成プログラム発行／認証サーバ, 12 登録ユーザ情報データベース, 35 液晶ディスプレイ, 82 ウェブブラウザ, 83 表示プログラム, 85 Java（登録商標）アプレット実行プログラム, 107 CCDカメラ, 109 液晶ディスプレイ, 192 サイバーコードファインダ, 193 認証プログラム, 222 Seed作成プログラム, 223 サイバーコード生成プログラム発行部, 224 認証用キー分離プログラム, 225 認証プログラム, 241, 242 サイバーコード

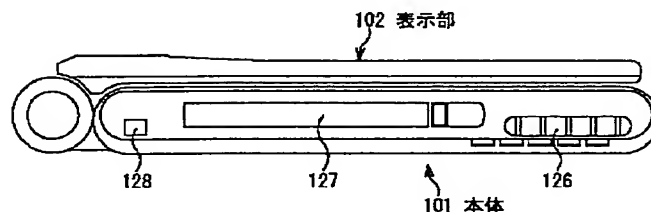
【図4】

図4

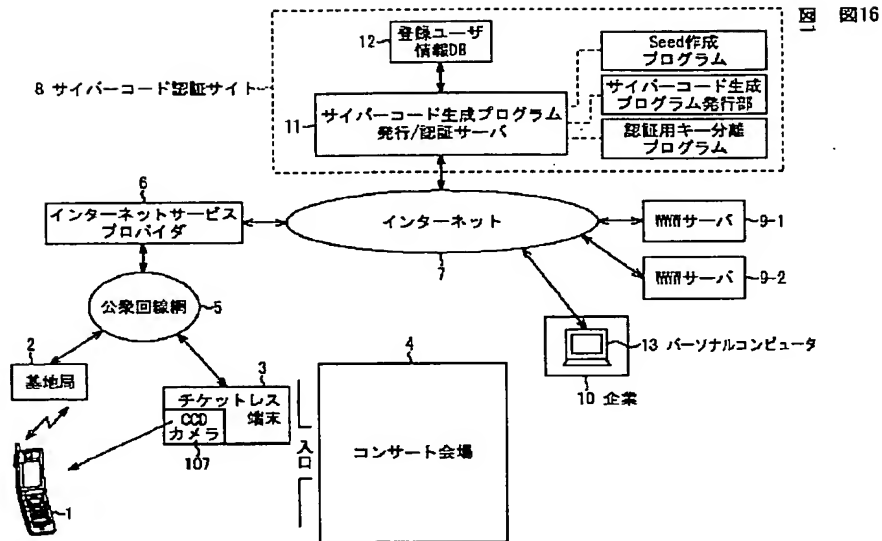


【図8】

図8



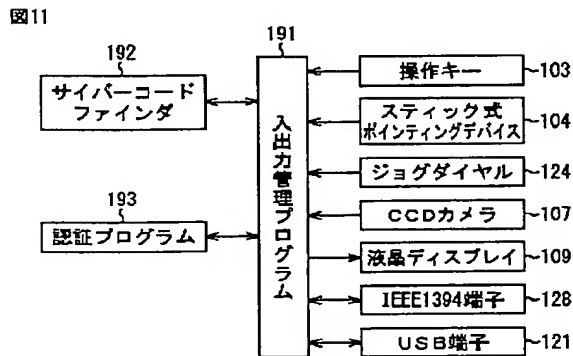
【図1】



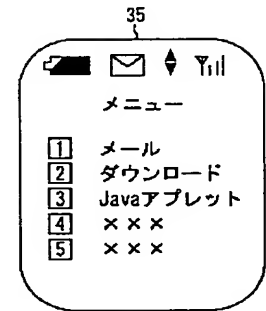
【図2】

氏名	ユーザID	発行開始時刻	乱数発生用Seed	ユーザ情報
山田〇〇〇	U001	T001	Seed001	
田中△△△	U002	T002	Seed002	.
鈴木×××	U003	T003	Seed003	.
.
.

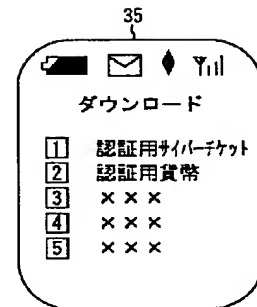
【図11】



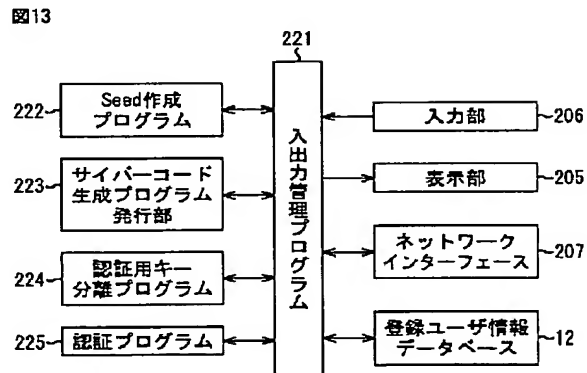
【図16】



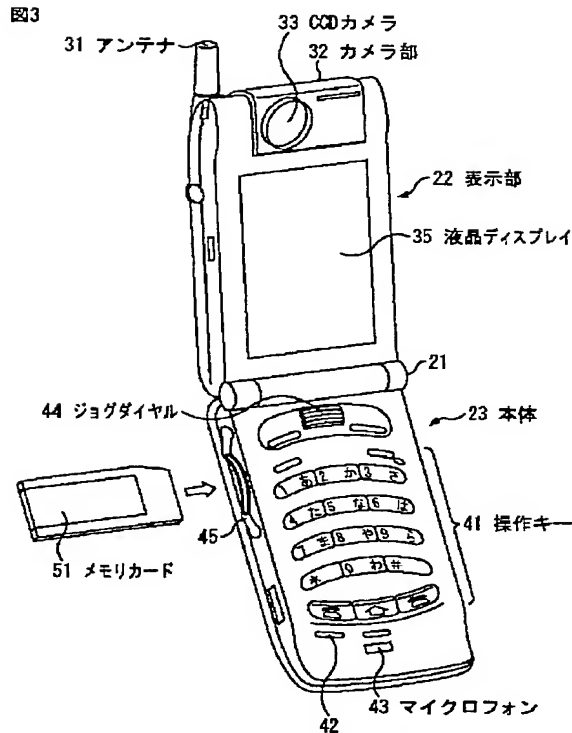
【図17】



【図13】

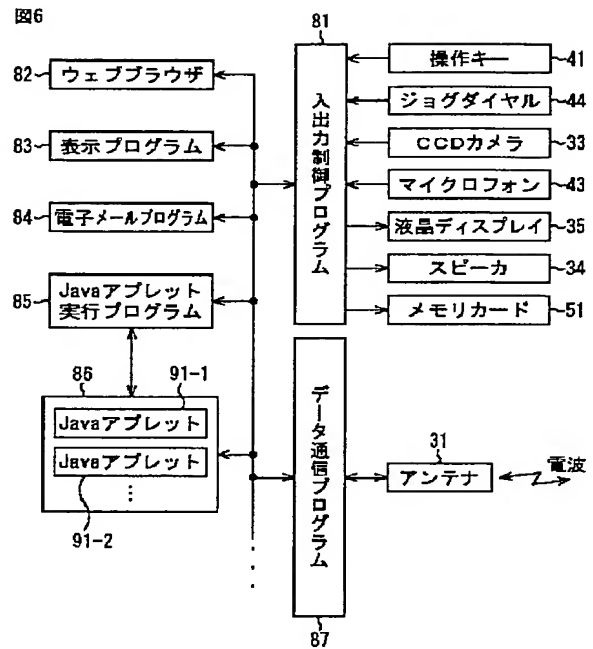


【図3】

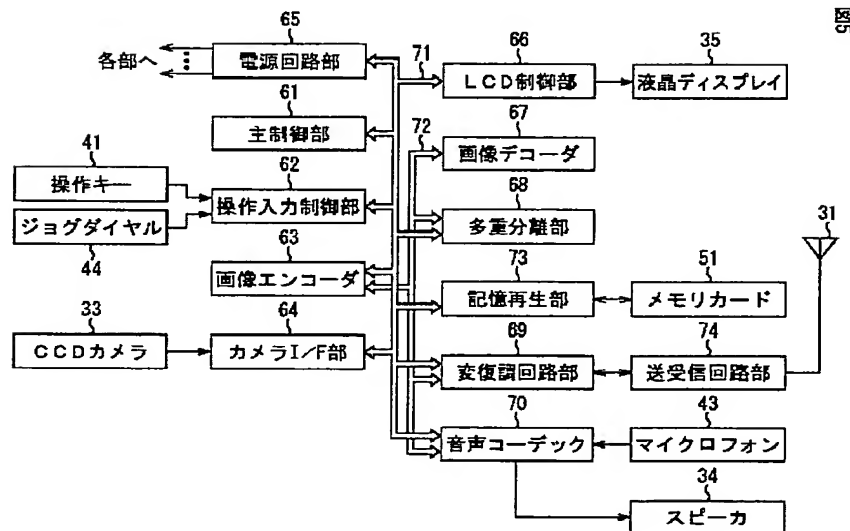


カメラ付デジタル携帯電話機 1

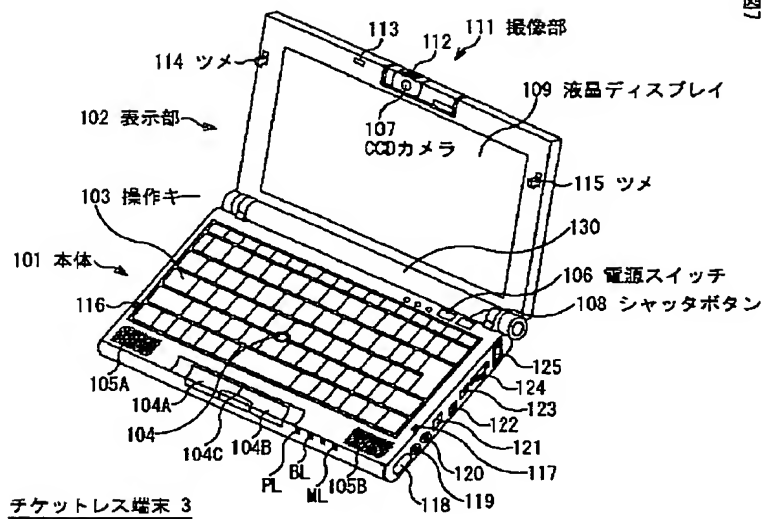
【図6】



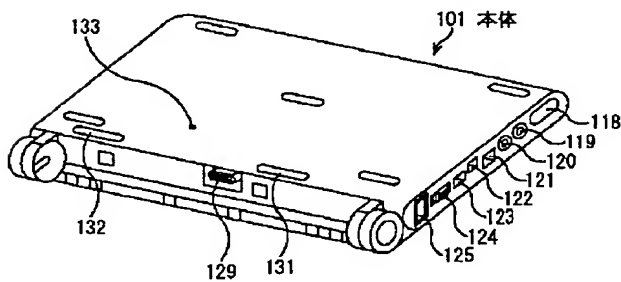
【図5】



【図7】

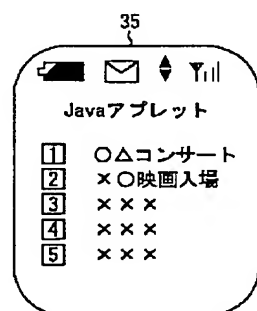


【図9】



【図21】

図21



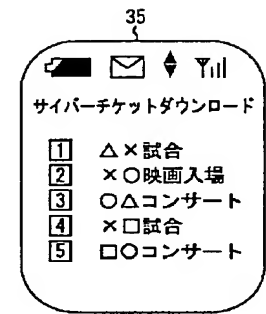
【図22】

図22



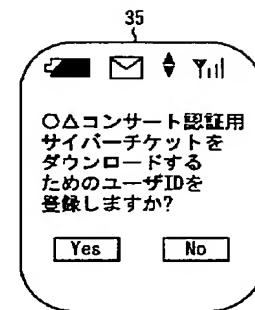
【図18】

図 18

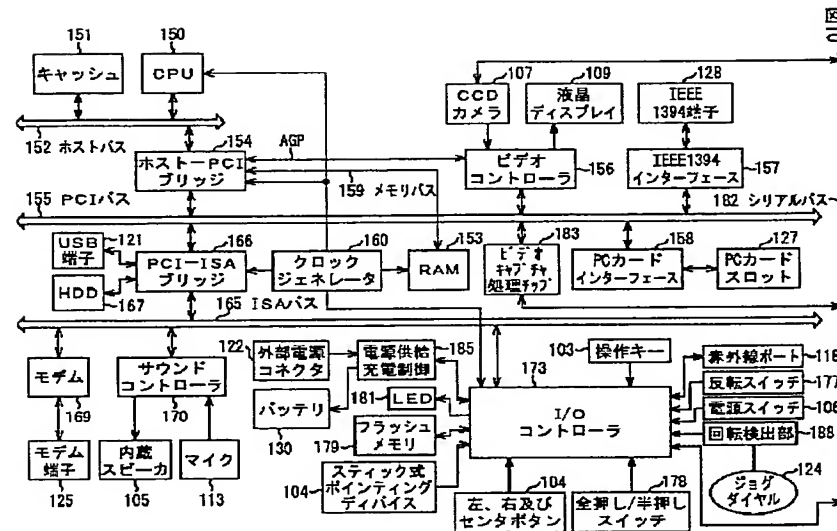


【図19】

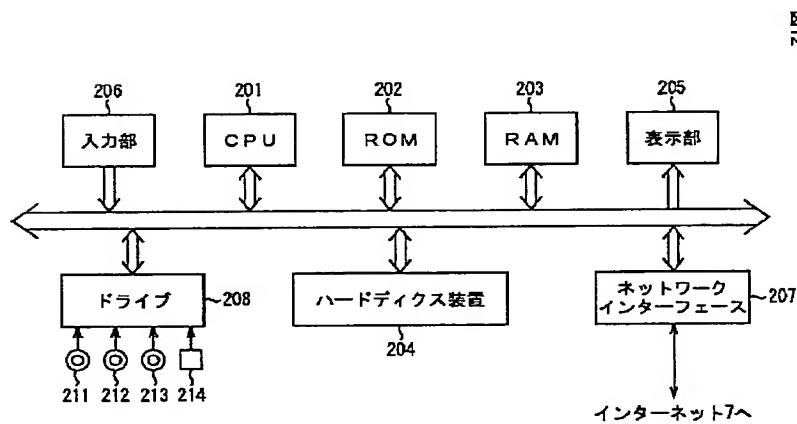
図 19



【図10】

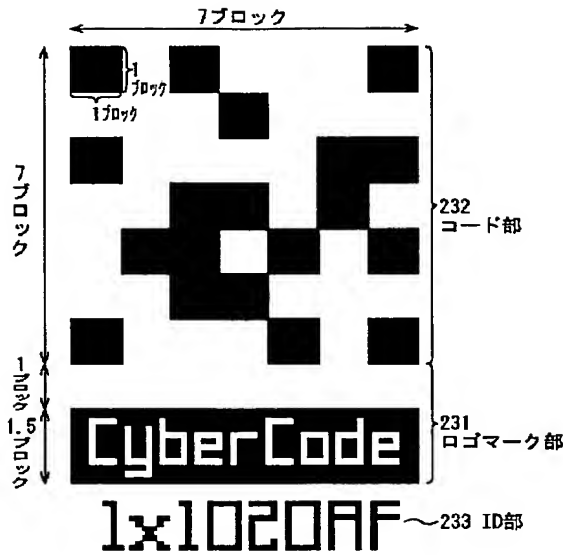


【図12】



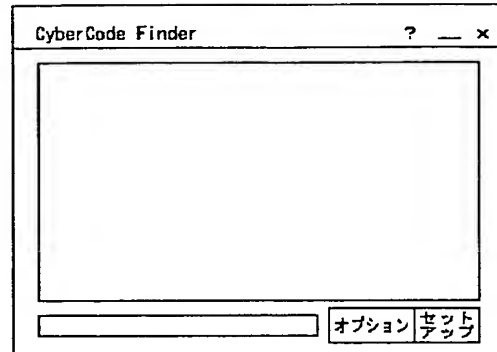
【図14】

図14

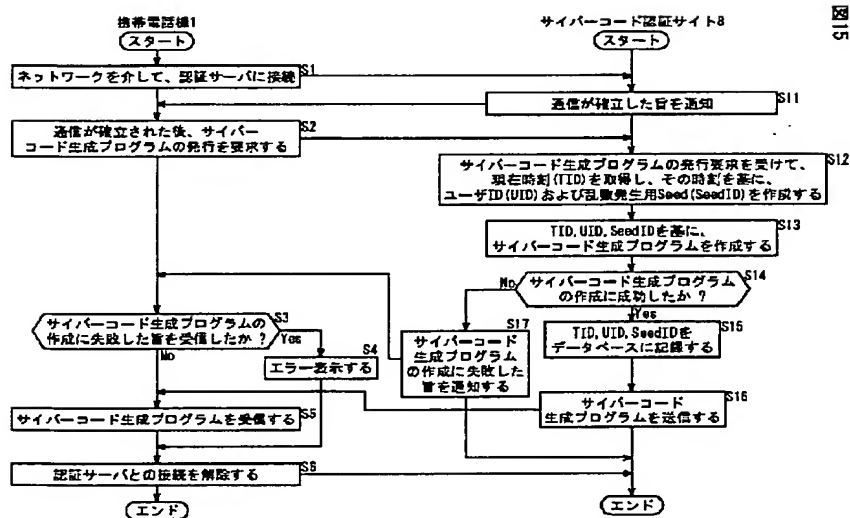


【図24】

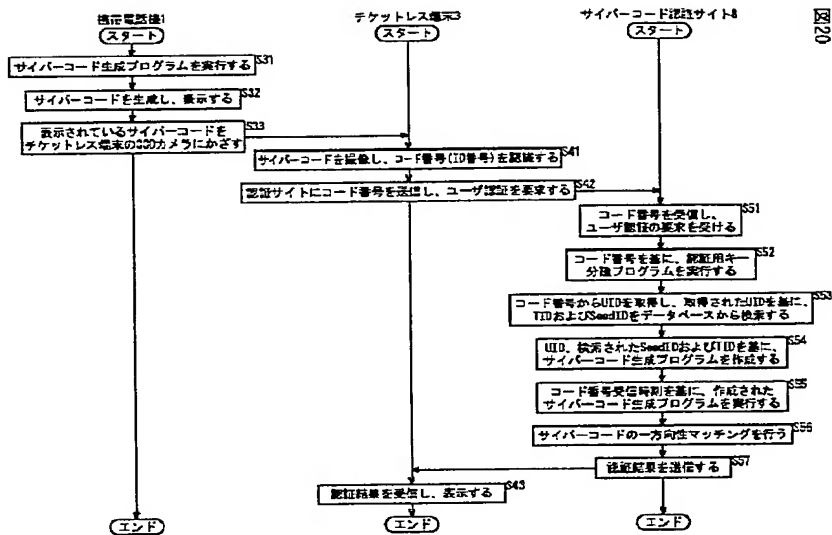
図24



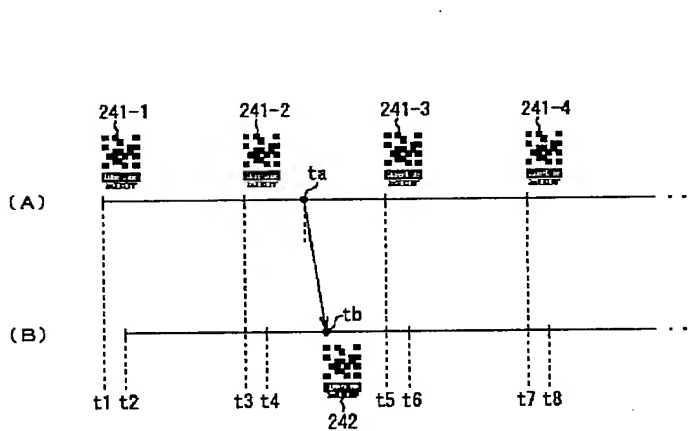
【図15】



【図 20】



【図 23】



【図 25】

【図 26】

図 25

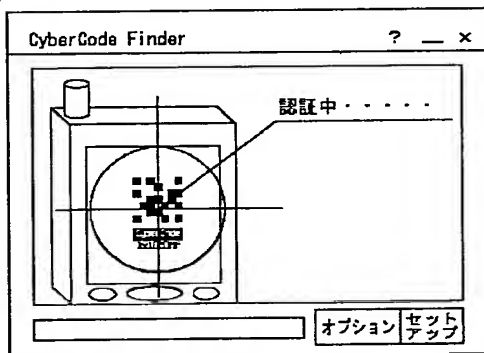
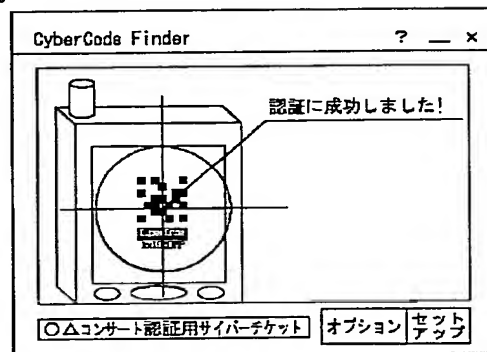
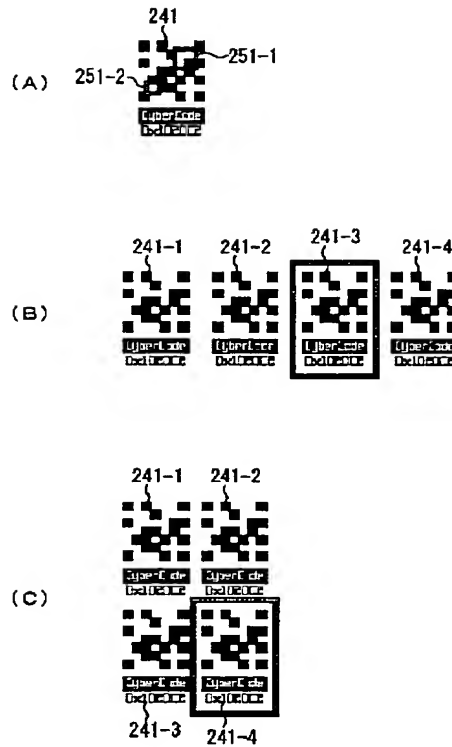


図 26



【図 2 7】

図27



フロントページの続き

(51) Int. Cl. ⁷ G 0 6 F 17/60	識別記号 5 0 6	F I H 0 4 L 9/00	テーマコード* (参考) 6 7 5 D 6 7 3 C
(72) 発明者 末吉 隆彦 東京都品川区北品川 6 丁目 7 番 35 号 ソニー株式会社内		(72) 発明者 松下 伸行 東京都品川区東五反田 3 丁目 14 番 13 号 株式会社ソニーコンピュータサイエンス研究所内	
(72) 発明者 綾塚 祐二 東京都品川区東五反田 3 丁目 14 番 13 号 株式会社ソニーコンピュータサイエンス研究所内		(72) 発明者 暦本 純一 東京都品川区東五反田 3 丁目 14 番 13 号 株式会社ソニーコンピュータサイエンス研究所内	
F ターム (参考) 5B017 AA06 BA07 BB09 BB10 CA15 5B085 AE01 AE08 BA07 BG07 5J104 AA07 BA07 GA03 GA05 KA01 KA04 MA01 NA04 NA35 NA41 NA43 PA02 PA10 PA11			

THIS PAGE LEFT BLANK